



**This electronic thesis or dissertation has been
downloaded from Explore Bristol Research,
<http://research-information.bristol.ac.uk>**

Author:

Fagade, Tesleem

Title:

A Multi-Domain Approach for Security Compliance, Insider Threat Modelling and Risk Management

General rights

Access to the thesis is subject to the Creative Commons Attribution - NonCommercial-No Derivatives 4.0 International Public License. A copy of this may be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>. This license sets out your rights and the restrictions that apply to your access to the thesis so it is important you read this before proceeding.

Take down policy

Some pages of this thesis may have been removed for copyright restrictions prior to having it been deposited in Explore Bristol Research. However, if you have discovered material within the thesis that you consider to be unlawful e.g. breaches of copyright (either yours or that of a third party) or any other law, including but not limited to those relating to patent, trademark, confidentiality, data protection, obscenity, defamation, libel, then please contact collections-metadata@bristol.ac.uk and include the following information in your message:

- Your contact details
- Bibliographic details for the item, including a URL
- An outline nature of the complaint

Your claim will be investigated and, where appropriate, the item in question will be removed from public view as soon as possible.

*A MULTI-DOMAIN APPROACH FOR
SECURITY COMPLIANCE, INSIDER THREAT
MODELLING AND RISK MANAGEMENT*



University of
BRISTOL

Tesleem Fagade

Department of Computer Science

University of Bristol

**This dissertation is submitted to the University of Bristol in accordance
with the requirements for the award of the degree of DOCTOR OF
PHILOSOPHY in the Faculty of Engineering.**

September 2018

Word Count: 43684

DEDICATION

This thesis is dedicated to my late Father, Alh. Hamzat Fagade

(The best man I ever knew)

PERSONAL STATEMENT OF QUOTE

I am an Eagle; I soar above the storm.

AUTHOR'S DECLARATION

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: DATE:

Tesleem Fagade

ABSTRACT

Information security is fundamentally concerned with the confidentiality, integrity and availability of information assets at all times. However, given the ubiquitous nature of information systems and organisations' growing reliance on large-scale interconnected networks; coupled with the increasing cyber-capabilities of adversaries, and widely available sophisticated hacking tools, it means that the prevalence and impact of cyber-attacks will continue to rise. Banking and financial organisations, in particular, operate in a dynamic and complex environment where risk management is an endless game between system defenders and adversaries. Therefore, given the complexity of cybersecurity and different layers of risks associated with this phenomenon, it has attracted a lot of interests from academic researchers, the private sector and government institutions.

The problem of cybersecurity risks management in corporate organisations is non-trivial, hence, constructing tools that truly satisfy the holistic management of information security is difficult and not readily available. The work described in this thesis presents a multi-domain approach to support comprehensive security management in organisations. This global objective is achieved through the evaluation of compliant security model and how employees rationalise security behaviour while using some ISO/IEC 27001 certified banking organisations as a regional case study. The study investigates the internal and contextual factors that drive individual security behaviour intentions. Based on the characteristics that have been proven to influence human behaviour, like personality traits, emotional states, psychosocial and cognitive capabilities, this work used values from these attributes in combination with security data breach reports, to develop a conceptual model that represents possible predictor of malicious insider activities. Also, in order to encapsulate the problems under consideration, this study explores organisations can optimise resource allocation for security investment; a feat that is often affected by intrinsically uncertain variables and

disparities in resource allocation decisions. The work presented in this thesis is based on the review of existing theories that are focused on human behaviour within the context of information security and criminology. The findings from this study also identified several factors that could strongly project the intention to violate security protocols, and the results significantly increase our understanding of the elements required in support of holistic security management. This study has implications for security professionals and organisational security management.

ACKNOWLEDGEMENTS

Firstly, I give all thanks and glory to God Almighty for seeing me through the four years of my PhD program; it is undeniably the most challenging period of my life on personal and professional levels. I am grateful for God's mercies that in the end, it is a worthy accomplishment.

I thank my Mother, Alh. Monishola Fagade and my Father, Alh. Hamzat Fagade (who sadly passed, few months before my thesis submission). My parents were the pillars and sources of motivation throughout the PhD program. Their prayers, support and unconditional love will never be forgotten.

Special gratitude goes to my supervisor who later became a friend, Dr Theo Tryfonas. His guidance, support, advice and friendship will always be cherished, especially, his relentless effort to get me going on our first publication.

I will like to thank late Alh. Musa Ujah, for starting me on this journey. A man who sees the potential in others and generously invest in people. I will always remember his goodwill.

Deepest appreciation to my jewels, Muna, Almaz and Jasmin for their support and understanding throughout the busy period of this study. Especially, Almaz, for her extraordinary display of maturity and support at my darkest hours. She is the reason why I get up and push ahead on several occasions. *Thank you so dearly, Sisi.*

Special thanks go to all my family; I am blessed to have them in my life. Importantly, the personal sacrifices and selflessness of Bunmi and Bola will forever be cherished. You are truly God sent sisters.

Finally, I will like to thank my research group and collaborators for their support. Dr Nabeel Albishry, Dr Theodoros Spyridopoulos, Dr George Oikonomou, Dr Panos Andriotis, Mr Konstantinos Maraslis, Mrs Fatmah Bamashmoos and Mr Adaraniyo Peters. I genuinely appreciate your help and advice; I could not have done this without you all.

LIST OF PUBLICATIONS

Journal Articles

- Fagade, T., Maraslis, K. and Tryfonas, T. (2017) 'Towards Effective Cybersecurity Resource Allocation: The Monte Carlo Predictive Modelling Approach', *International Journal of Critical Infrastructures*, 13(2/3), p. 152. doi: 10.1504/IJCIS.2017.088235.
- Fagade, T. and Tryfonas, T. (2017a) 'Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization', *Journal on Systemics, Cybernetics and Informatics: JSCI*, 15(Number 5), pp. 74–80.

Conference Proceedings

- Fagade, T. and Tryfonas, T. (2017c) 'Malicious Insider Threat Detection: A Conceptual Model', in Jaroslav Dockal, Milan Jirsa, and Josef Kaderka (eds) *Security and Protection of Information 2017*. Brno: University of Defence, IDET, pp. 31–44.
- Fagade, T., Spyridopoulos, T., Albishry, N. and Tryfonas, T. (2017) 'System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis', in Tryfonas T. (ed.) *Human Aspects of Information Security, Privacy and Trust. HAS 2017, Lecture Notes in Computer Science*, Springer, Cham, pp. 309–321. doi: 10.1007/978-3-319-58460-7_21.
- Fagade, T. and Tryfonas, T. (2017b) 'Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization', in: Nagib Callaos, Elina Gaile-Sarkane, Shigehiro Hashimoto, Natalja Lace, and Belkis Sanchez (eds) *Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017)*, vol. 2. Orlando, Florida: International Institute of Informatics and Systemics, Winter Garden, Florida. ISBN 978-1-941763-60-5, pp. 94–99.

-
- Fagade, T. and Tryfonas, T. (2016) ‘Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks’, in Tryfonas T. (eds), *Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science. Toronto, Canada*: Springer, Cham, pp. 128–139. doi: 10.1007/978-3-319-39381-0_12.
 - Nabeel Albishry, Tom Crick, Theo Tryfonas, and Tesleem Fagade. (2018.) An Evaluation of Performance and Competition in Customer Services on Twitter: A UK Telecoms Case Study. In *WWW ’18 Companion: The 2018 Web Conference Companion, April 23–27, 2018, Lyon, France*. ACM, New York, NY, USA, 1-8 pages. <https://doi.org/10.1145/3184558.3191631>
 - Albishry, N, Crick, T, Fagade, T & Tryfonas, T, 2018, ‘Popularity and Geospatial Spread of Trends on Twitter: A Middle Eastern Case Study’. in: Proceedings of the 10th International Conference on Computational Collective Intelligence (ICCCI 2018): 5-7 September 2018 - Bristol, UK. Springer

Working papers.

- Tesleem Fagade, Theo Tryfonas, Nabeel Albishry “TP-UBA Approach for a Better Security Compliance”. International Conference on Emerging Trends in Engineering & Technology on Information Security and Analytics (ICETET- ISA) 2018.

Poster Presentations (see Appendices II and III)

- Fagade, T. and Tryfonas, T. “Cybersecurity Resource Allocation: The Monte Carlo Predictive Modelling Approach”. *The Information Assurance Advisory Council (IAAC) Symposium*, 15th September 2016, BT Centre auditorium London.
- Fagade, T. and Tryfonas, T. “A Conceptual Model of Malicious Insider Threat Detection” *Joint UK and Israel Cyber Security Workshop*, 12-13 March 2018. University of Kent, Canterbury Campus. U.K.

LIST OF ABBREVIATIONS AND ACRONYMS

ABC	Activity-Based Costing
AHP	Analytic Hierarchy Process
ALE	Annual Loss Expectancy
AVE	Average Variance Extracted
BCP	Business Continuity Plan
BIA	Business Impact Analysis
brisk-I	Behavioural Risk Indicators
BV	Blaming the Victim
CBN	Central Bank of Nigeria
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Cmax	Maximum Cost
Cmin	Minimum Cost
Cml	Most-Likely Cost
CNI	Critical National Infrastructure
COBIT	Control Objectives for Information and Related Technologies
CSF	Cyber-Security Framework
DAC	Discretionary Access Control
DAS	DDoS Mitigation System
DDoS	Distributed Denial of Service
DI	Denial of Injury
DR	Denial of Responsibility
EEG	Electroencephalography

fMRI	functional magnetic resonance imaging
GLBA	Gramm-Leach Bliley Act
HIPPA	Health Insurance Portability and Accountability Act
HKMA	Hong Kong Monetary Authority
HR	Human resource
ICO	Information Commission Office
ICS	Industrial Control System
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Committee
IoT	Internet of Things
IS	Information Security
ISA	Information Security Architecture
ISMS	Information Security Management System
ISO	International Organization for Standardization
KA	Knowledge and Awareness
LIWC	Linguistic Inquiry and Word Count
LRE	Low sense of response efficacy
LSS	Low sense of sanction severity
LTV	Low sense of threat vulnerability
MAC	Mandatory Access Control
MATLAB	Matrix Laboratory
MBTI	Myers-Briggs Type Indicator
NEO-PI-R	Revised Neuroticism-Extraversion-Openness Personality Inventory
NGO	Non-Governmental Organisations

NIST	National Institute of Standards and Technology
NITDA	National Information Technology Development Agency
OCEAN	Openness, Conscientiousness, Extroverted, Agreeable and Neuroticism
PCDA	Plan-Do-Check-Act
PCI DSS	Payment Card Industry Data Security Standard
PLS-SEM	Partial Least Squares Structural Equation Modelling
prisk-I	Personality Risk Indicators
PMT	Protective Motivation Theory
PS	Psychological State
R.S.	Risk Score
R.T.	Risk Threshold
RAPSA	Risk Analysis and Probabilistic Survivability Assessment
Re	Risk Elements
ReW	Risk Element Weights
ROI	Return on Investment
ROSI	Return on Security Investment
RPAC	Role-Based Access Control
SC	Security Culture
SIEM	Security Information and Event Management
TPB	Theory of Planned Behaviours
trisk-I	Technical Risk Indicators
VENSIM-PLE	Ventana Systems Simulation Personal Learning Edition
VSM	Viable System Model

CONTENTS

DEDICATION.....	I
PERSONAL STATEMENT OF QUOTE	III
AUTHOR'S DECLARATION	V
ABSTRACT	VII
ACKNOWLEDGEMENTS.....	XI
LIST OF PUBLICATIONS	XIII
LIST OF ABBREVIATIONS AND ACRONYMS	XVII
CONTENTS.....	XXI
LIST OF TABLES.....	XXVII
LIST OF FIGURES.....	XXIX
LIST OF APPENDICES.....	XXXI
1 INTRODUCTION	1
1.1 INTRODUCTION	2
1.2 OVERVIEW OF THE RESEARCH PROBLEM	4
1.3 RESEARCH MOTIVATION	6
1.3.1 <i>Security Standards and Compliance</i>	7
1.3.2 <i>Malicious Insider Threats</i>	8
1.3.3 <i>Resource Allocation for Information Security Investment</i>	8
1.4 RESEARCH QUESTION	9
1.5 THESIS STRUCTURE	11
SECTION 1: INFORMATION SECURITY RISK MODELLING, STANDARDIZATION AND COMPLIANCE IN BANKING ORGANISATIONS. 17	
2 LITERATURE REVIEW.....	19
2.1 INTRODUCTION	20
2.2 INFORMATION SECURITY STANDARDIZATION AND COMPLIANCE	22
2.2.1 <i>Framework for Information Security Standards</i>	22
2.2.2 <i>The PCDA Compliance Model</i>	27
2.2.3 <i>Information Security Cultural Framework</i>	28
2.2.4 <i>Information Security Risk Metrics</i>	33
2.2.5 <i>Organisation Security Compliance Challenges</i>	35

2.3 INSIDER THREATS: THEORETICAL, BEHAVIOURAL, MODELLING AND SIMULATION PERSPECTIVES.....	37
2.3.1 Threat Agents.....	38
2.3.2 Threat Vectors.....	39
2.3.3 Insiders' Theoretical Frame of Reference.....	42
2.3.4 Insiders' Behavioural Frame of Reference.....	46
2.3.5 Modelling and Simulation.....	49
2.4 RISK ASSESSMENT, INCENTIVES AND RESOURCE ALLOCATION.....	50
2.4.1 Appropriating Security Risks.....	51
2.4.2 Misaligned Incentives.....	53
2.4.3 Allocating Resources for Security Investment.....	54
2.4.4 Some Prima on Interdependent Decisions and the Game Theory.....	58
2.5 GAPS IN THE LITERATURE.....	61
2.6 CONCLUSION.....	64
3 RESEARCH DESIGN.....	69
3.1 INTRODUCTION.....	70
3.2 RESEARCH QUESTION.....	71
3.3 RESEARCH METHODOLOGY.....	76
3.3.1 Qualitative and Quantitative Research Approach.....	77
3.3.2 Modelling and Simulation-Based Approach.....	80
3.4 RESEARCH ETHICS.....	82
3.5 CONCLUSION.....	82
SECTION 2: DEVELOPED METHODS AND MODELS.....	85
4 SECURITY BY COMPLIANCE AND THE IMPLICATIONS FOR BANKING ORGANISATIONS.....	87
4.1 INTRODUCTION.....	88
4.2 RESEARCH METHOD.....	89
4.2.1 Case Selection.....	89
4.2.2 Data Collection.....	90
4.2.3 Sample Demography.....	91
4.2.4 Survey Development.....	92
4.3 RESULTS AND ANALYSIS.....	94

4.4 EMBEDDING SECURITY IN ORGANIZATIONAL CULTURE.....	96
4.4.1 <i>Compliance Gap Mitigation: Data Security Scenario</i>	97
4.5 CONCLUSION	101
5 EXPLORATORY STUDY OF COMPLIANCE-BASED INFORMATION SECURITY MANAGEMENT IN BANKING ORGANISATIONS	105
5.1 INTRODUCTION	107
5.2 THEORY DEVELOPMENT	108
5.3 RESEARCH MODEL AND HYPOTHESES	110
5.3.1 <i>The Role of Personality Traits and Security Scenario Effects</i>	110
5.3.2 <i>The Role of Neutralization Techniques</i>	111
5.3.3 <i>The Role of Information Security Culture, Knowledge and Awareness</i>	113
5.4 RESEARCH METHOD.....	113
5.4.1 <i>Survey Development</i>	113
5.4.2 <i>Validation of Measurement</i>	114
5.4.3 <i>Structural Model Analysis</i>	116
5.5 DISCUSSION OF RESULTS	117
5.6 CONCLUSION	118
6 SYSTEM DYNAMICS APPROACH TO MALICIOUS INSIDER CYBER- THREAT MODELLING AND ANALYSIS.....	121
6.1 INTRODUCTION	122
6.1.1 <i>Why System Dynamic Models?</i>	122
6.2 OVERVIEW OF MODEL INTERCONNECTED RISK DOMAINS.....	123
6.2.1 <i>Personality Risk Indicators</i>	124
6.2.2 <i>Behavioural Risk Indicators</i>	127
6.2.3 <i>Technical Risk Indicators</i>	129
6.3 METHODOLOGY AND SIMULATION ENVIRONMENT	130
6.3.1 <i>Model Analysis</i>	130
6.3.2 <i>Model Results and Discussion</i>	132
6.4 CONCLUSION	135
7 MALICIOUS INSIDER THREAT DETECTION: A CONCEPTUAL MODEL	139
7.1 INTRODUCTION	140

7.2 BACKGROUND DESCRIPTION OF THE CONCEPTUAL MODEL	141
7.2.1 <i>Personality Risk Factors</i>	142
7.2.2 <i>Technical Risk Factors</i>	142
7.2.3 <i>Behavioural Risk Factors</i>	143
7.3 METHOD AND PRELIMINARY DESIGN.....	144
7.4 SIMULATION RESULT AND DISCUSSION.....	148
7.5 CONCLUSION.....	149
8 INCENTIVES AND SECURITY INVESTMENT DECISIONS IN INFORMATION SECURITY.....	153
8.1 INTRODUCTION	154
8.2 RISK MANAGEMENT OVERVIEW	155
8.3 A BACKGROUND DESCRIPTION OF OUR PREDICTIVE MODEL	157
8.3.1 <i>Different Approaches to Resource Allocation Decision Processes....</i>	157
8.3.2 <i>Deterministic Estimation of Security Breach Costs</i>	160
8.3.3 <i>Probabilistic estimation of security breach costs.....</i>	163
8.4 METHODOLOGY.....	164
8.5 SIMULATION RESULT AND DISCUSSION.....	167
8.6 CONCLUSION.....	169
SECTION 3: CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK....	173
9 RESEARCH FINDINGS AND FUTURE WORK.....	175
9.1 CONCLUSION.....	176
9.2 FINDINGS	178
9.3 CONTRIBUTIONS	180
9.4 LIMITATIONS	182
9.5 DIRECTIONS FOR FUTURE WORK.....	184
REFERENCES.....	187
APPENDICES	215
APPENDIX I: CONCEPTS AND DEFINITIONS.....	217
APPENDIX II: INTERVIEW QUESTIONS.....	221
APPENDIX III: SURVEY QUESTIONS	222
APPENDIX IV: SURVEY MEASUREMENT MODEL - A	223
APPENDIX V: RECRUITMENT INFORMATION	224

APPENDIX VI: CLOSED ONLINE GOOGLE FORM.....	225
APPENDIX VII: SURVEY MEASUREMENT MODEL - B	226
APPENDIX VIII: IAAC 2016 POSTER	227
APPENDIX IX: CSW 2018 POSTER.....	228
APPENDIX X: THESIS TEMPLATE	229

LIST OF TABLES

TABLE 2.1. ISO27001 CONTROL OBJECTIVES (DISTERER,2013)	24
TABLE 2.2. COUNTRY RANKINGS BASED ON THE OVERALL ISO CERTIFICATE ISSUED (ISO, 2017).....	25
TABLE 2.3. PERSONALITY DIMENSIONS MEASURED BY THE NEO PI-R [47].....	45
TABLE 2.4. DEFINITION OF SITUATIONAL FACTOR (MCBRIDE, 2012).....	46
TABLE 4.1. DATA COLLECTION STAGES	90
TABLE 4.2. EXTRACTS FROM THE ONLINE INFORMATION SECURITY SURVEY.....	93
TABLE 5.1. CROSS-LEVEL INTERACTION BETWEEN PERSONALITY TRAITS AND SECURITY SCENARIO EFFECTS (MCBRIDE, 2012)	110
TABLE 5.2. LATENT VARIABLES VALIDITY AND RELIABILITY MEASUREMENT	114
TABLE 5.3. FINDINGS ON STRUCTURAL RELATIONSHIP SHOWING PATH LOADINGS AND T-VALUES.....	116
TABLE 6.1. THE BIG FIVE PERSONALITY TRAITS AND SECURITY SCENARIO EFFECTS (MCBRIDE, 2012).....	125
TABLE 6.2. PSYCHOSOCIAL RISK INDICATORS (GREITZER, 2010)	128
TABLE 7.1. RISK INDICATORS.....	141
TABLE 7.2. RISK ELEMENTS.....	146
TABLE 7.3. HIGH-LEVEL ALGORITHM FOR THE MALICIOUS INSIDER THREAT DETECTION	147
TABLE 8.1. RISK LIKELIHOOD AND SEVERITY	160
TABLE 8.2. RISK RATING TABLE.....	162
TABLE 8.3. EXPERT ESTIMATION OF SECURITY BREACH COSTS	162
TABLE 8.4 MODEL SIMULATION PARAMETERS.....	164

LIST OF FIGURES

FIGURE 1.1 THESIS STRUCTURE.....	13
FIGURE 2.1. NUMBER OF ISO27001 CERTIFICATES ISSUED GLOBALLY (IRWIN, 2017) ...	26
FIGURE 2.2. PCDA MODEL APPLIED TO ISMS PROCESSES (BSI, 2002)	27
FIGURE 2.3. ANTECEDENTS OF SECURE BEHAVIOUR (RENAUD, 2014)	29
FIGURE 2.4. INFORMATION SECURITY GOVERNANCE FRAMEWORK (HUMPHREYS, 2008)	31
FIGURE 2.5. SECURITY METRICS AS MANAGEMENT’S DECISION-MAKING TOOL (VOGEL, 2017).....	34
FIGURE 2.6. THREAT VECTOR BY INDUSTRY (CLIVE, 2016)	40
FIGURE 3.1. A HIGH-LEVEL OVERVIEW OF THE RESEARCH PROCESS	70
FIGURE 3.2. RESEARCH QUESTIONS	72
FIGURE 3.3. A LOW-LEVEL OVERVIEW OF THE RESEARCH PROCESS.....	73
FIGURE 4.1. DEMOGRAPHY OF RESPONDENTS	95
FIGURE 4.2. INFORMATION SECURITY COMPLIANCE RESULTS	95
FIGURE 4.3. SECURITY CULTURE INTEGRATION CONCEPT	98
FIGURE 5.1. STRUCTURAL EQUATION MODEL RESULTS	115
FIGURE 6.1. CYBERSECURITY RISK REDUCES DUE TO PERSONALITY TRAITS UNDER SPECIFIED CONDITIONS.....	126
FIGURE 6.2. CYBERSECURITY RISK INCREASES DUE TO PERSONALITY TRAITS UNDER SPECIFIED CONDITIONS	126
FIGURE 6.3. CYBERSECURITY RISK INCREASES DUE TO INDIVIDUAL’S BEHAVIOUR OR EXTERNAL INFLUENCE WITH NEGATIVE PSYCHOLOGICAL EFFECTS	129
FIGURE 6.4. HIGH-LEVEL ABSTRACTION OF THE INSIDER THREAT MODELLING PROCESS.	131
FIGURE 6.5. DYNAMIC RELATIONSHIP BETWEEN PERSONALITY, BEHAVIOUR AND CYBER- SECURITY INCIDENT	133

FIGURE 6.6. PROBABILITY OF DATA CORRUPTION IN TIME BASED ON PERSONALITY	134
FIGURE 6.7. PROBABILITY OF DATA CORRUPTION IN TIME BASED ON BEHAVIOUR.....	134
FIGURE 7.1. HIGH-LEVEL ABSTRACTION OF THE INSIDER THREAT MODELLING.....	145
FIGURE 7.2. SIMULATION OUTPUT SHOWING HOW TO DETECT MALICIOUS INSIDER ACTIVITIES FROM MULTIPLE RISK INDICATORS.....	148
FIGURE 8.1. HIGH-LEVEL CONCEPTUAL MODEL DIAGRAM.....	158
FIGURE 8.2. LOW-LEVEL CONCEPTUAL MODEL DIAGRAM SHOWING KEY ASSET POINTS ...	159
FIGURE 8.3. SCHEMA OF THE MC PREDICTIVE MODEL	165
FIGURE 8.4. SIMULATION RESULT IN 'MODELRisk' WITH CUMULATIVE OVERLAY.....	167
FIGURE 8.5. SIMULATION RESULT IN MATLAB SHOWING VALUES FOR C_{MIN} AND C_{MAX} ...	168

LIST OF APPENDICES

APPENDIX I: CONCEPTS AND DEFINITIONS	217
APPENDIX II: INTERVIEW QUESTIONS.....	221
APPENDIX III: SURVEY QUESTIONS.....	222
APPENDIX IV: SURVEY MEASUREMENT MODEL - A	223
APPENDIX V: RECRUITMENT INFORMATION.....	224
APPENDIX VI: CLOSED ONLINE GOOGLE FORM.....	225
APPENDIX VII: SURVEY MEASUREMENT MODEL - B.....	226
APPENDIX VIII: IAAC 2016 POSTER	227
APPENDIX IX: CSW 2018 POSTER	228
APPENDIX X: THESIS TEMPLATE.....	229

1 INTRODUCTION

"If security were all that mattered, computers would never be turned on, let alone hooked into a network with literally millions of potential intruders."

-Dan Farmer

This introductory chapter sets the tone for the rest of the thesis by presenting an overview of the problem, the research motivation and the research questions in this study. Important issues of security compliance, the insider threat and resource allocation for security investment are also covered in relation to the challenges of identifying, defending and pre-empting security threats in organisations. Finally, the thesis structure, scope and outlines are presented in the closing section of this chapter.

1.1 Introduction

Organizations' information systems are increasingly subjected to the risks that come with businesses reliance on technology, in terms of information processing, storage and dissemination. The digital gap between businesses with respect to people and systems is generally becoming ubiquitous due to technology advancement and the seamless human-machine interaction that has been integrated along the business process evolution [1]. In particular, the dynamics of modern-day economies, and how information is created and distribute requires that organisations are dependent on large-scale interconnected information systems, which also leads to increased cyber-risk exposure [2].

Risk management is a critical issue for most organisations. Not only are organisations' reliance on large-scale interconnected information assets on the increase, but the widely available sophisticated attacker tools also suggest that the prevalence and impact of cyber-attacks are set for a rapid increase as well [3]. Hence, cybersecurity is one of the most significant challenges facing businesses in recent times. Economic loss due to cyber-attack is on the increase, and many businesses have been obliterated due to loss of intellectual assets to cybercriminals. This figure is set to grow exponentially, according to the study conducted in [4] which enunciated that by 2020, losses from cyber-attack may hit the \$20 trillion mark. In a different report [5], studies conducted to quantify the actual and potential value of losses as a result of successful system breaches are put in the region of \$500 million and \$5 billion per year in the USA alone. Therefore, the importance of risk management cannot be overemphasised.

Information security management policies are often difficult to be successfully implemented because significant issues of diffused liability and incentives are not appropriately distributed. Information systems exploitation is not always a consequence of technical or policy failure, but often due to the lack of balanced incentives between the designers and users of such systems [6]. Despite managements' efforts to protect organisation data, problems of identity theft, database breaches and stolen passwords continue to be the

crucial challenges faced by corporate organisations and government agencies [7]. In today's cyber battle, an agent's elevated access to information and services creates potential vulnerability to the system, signifying possible issues of malicious insider activities. One of the most significant challenges faced by organisations is system misuse by trusted insiders, whose actions are deeply rooted in non-compliance. It is one thing for organisations to meet the demands of regulatory standards, but it is a different challenge to enforce compliance behaviour within a workforce. As suggested in the relevant literature, insiders are the weakest link in organisations' security efforts [8],[9]; a system is more susceptible to insider threats exploitations compared to exploitations due to failures of technical and procedural measures. Thereby, implying that the most considerable threats come from insiders. Lack of compliance by employees to information security policies is claimed to be responsible for more than half of information systems security breaches [10]. It is often difficult for organisations to balance the psychological, incentive and communication need of employees as they interact with information systems, due to the complex nature of human behaviour. If all end users are rational, cybersecurity will be a straight game between defenders and attackers of information assets.

There are a lot of fundamental issues associated with risk evaluation, reporting and mitigation in the cybersecurity domain. The problem of cybersecurity risks management in corporate organisations is non-trivial, hence, constructing tools that genuinely satisfy every aspect of risk management and measurement theory is difficult; but also not readily available [11]. Information security is fundamentally concerned with the confidentiality, integrity and availability of information assets at all times. In order to defend against threats to information assets, organisations invest in countermeasures, however, as the number of assets to be protected grows and IT budgets are constrained, there is a need for careful evaluation of information security investments [12]. As firms' vulnerability to cyber-attacks increases, so is the need for further investment in cybersecurity enhancement

measures. Security managers can effectively reduce the potential and probability of loss to cyber rogues by reinforcing firms' cyber capabilities [13].

Finally, cybersecurity risk management is not only confined within the elements of compliance and the insiders' problem but also include the issues associated with optimum resource allocation for security investment. These three elements are valid problems as identified in the literature review in chapter two and form the basis of this study.

1.2 Overview of the Research Problem

An organization's continual effort to reinforce its cyber resilience and the unique challenge posed by malicious insiders, borders on issues that encompasses different loosely coupled variables; people, process, regulation and resources. Even more so, constructing tools to address these issues often involve several controls like technical, procedural, formal and informal solutions, which are difficult to apply in large and complex systems [14]. In reality, what constitutes information security risk, is relative to an organisation risk acceptance level. However, in most cases, security managers' priority is to mitigate organisational risk exposure that could undermine the confidentiality, integrity and availability of mission-critical systems at all levels.

Apart from huge financial losses to organisations, a security breach can lead to sanctions from industry regulators, negative corporate image, and loss of confidence in clients and customers [15]. A classic example is the case of TalkTalk, the UK communication giant that was hacked in 2015. Personal details of nearly 157,000 TalkTalk customers were accessed through a basic SQL injection attack on the company website. More than 15,000 personal account numbers and sort code were also stolen. The impact of cyber-attack is reported [16], [17] to have cost the company £42m, loss of over 100,000 customers and a fine of £400,000 for the data breach by the Information Commission Office (ICO). The ICO claimed that hacks could have been prevented if TalkTalk had implemented basic cybersecurity measures to

safeguard its customers' data. This shows that the problems associated with security compliance are still valid.

There are many drivers that can be considered when implementing organisations' Information Security Management System (ISMS); some of which can be evaluated from the perspective of compliance (focusing on regulations), insider threat (focusing on people) and security investment decisions (focusing on resources). In terms of regulations and standards like the ISO/IEC27001 Standard for best practices in ISMS, which outline general requirements for safeguarding organisations information assets. It defines the baseline requirements and controls for the assessment of ISMS, under the principle of confidentiality, integrity and availability [18]. However, the problem with Standards and security guidelines is that the thought process of system adversaries is not necessarily addressed. There seem to be a more concerted effort on the implementation of physical, policy and technical measures to mitigate anticipatory threats [19]. Furthermore, some of the previous research on this subject [20] also identified that Standards come with a predetermined set of guidelines for compliance. However, the size and need of organisations vary when it comes to protecting IT infrastructure. Different organisations require different security treatments. Hence, the one-cap-fits-all approach entrenched in Standards may undermine the effectiveness of security by compliance. Yet, this command-and-control approach is still taken by a large number of organisations [21]. Even much so, Standards are based on the principle of deterrence, which expects that employee's behaviour fits within a certain frame of reference [22], whereas, policies and procedures are behaviour oriented, and there is no absolute certainty that people always do as told. Therefore, security stakeholders always strive to know what the key drivers for non-compliance are.

In terms of Malicious Insiders, the dawn of web 3.0 (semantic web) and the mobile workforce also brings along a radical dimension to organisations information security problems. Insider threat manifests when agents' behaviour is contrary to regulatory policies and guidelines. It refers to harmful acts that a trusted employee may carry out to undermine the

confidentiality, integrity and availability of information assets [23]. Currently, there is no complete, effective and systemic method developed to address cybersecurity challenges [24]. Although, a lot of academic contributions have identified the central role of insiders in any fortified and secured environment, as stated in section 1.1, but the number of attempts to address human factors in cybersecurity is quite low despite the evidence suggesting that a malicious insider exhibits observable ‘concerning behaviour’ in advance of an exploit [24]. The problem space of insider threat continues to be valid, and researchers still seek answers to these problems [25].

In terms of resource allocation for cyber risk investment, it is difficult to estimate the financial impact of the insider problem because a lot of organisations fail to report insider misuse [26]. In addition, incentivising security investment is hard, partly because stakeholders’ perspectives on how to manage organisations cybersecurity initiative often differs when it comes to incentives and business motives. The perverse incentive has implications in many aspects of information security especially when those entrusted with the protection of information systems are not the ones that bear the consequences of security failure [27]. Hence, the challenge is how to design a system that can support security managers when making a business case for security investment. The problem areas of this work are focused on organisation security management challenges in respect to; information security compliance, predicting insiders’ intention to violate security protocols and optimisation of resource allocation for organisations’ cybersecurity investment.

1.3 Research Motivation

The three motivation elements of this work are based on factors that may undermine the cyber risk management of corporate organisations. Over the past decade, I have been actively involved in risk assessment as part of my studies and work. My Master’s thesis was based on risk assessment for critical infrastructures; where risk management is evaluated against the backdrop of standardisation and automated software. The motivation for the current study

centres on distinct areas that supports a more holistic approach to security management. The literature review is therefore confined to the scope of the research motivation, from which research gaps are identified, and research questions are developed. In the following sub-sections, each element is briefly discussed to set the tone for the rest of the thesis.

1.3.1 Security Standards and Compliance

The first motivation for this study stems from the directives issued to all banking organisations in Nigeria by the Central Bank of Nigeria (CBN). The CBN is the apex bank responsible for monitoring, reforming and regulating the activities of banks and other financial institutions in Nigeria [28]. The CBN mandated that all Nigerian banks must be ISO/IEC 27001 certified by December 2015 or run the risk of sanctions. The certification is mostly conducted by third-party accredited assessors, and the Ultima Risk Management (URM) [29], a UK risk management company, conducted the certification process for most of the Nigerian banks. Hence, by the end of 2015, all the major banks in Nigeria have been ISO/IEC 27001 certified.

If an organisation complies with policy, law, regulation or a legally binding necessity identified with information security, then the organisation's information security program may suggest that is consistent with all the prerequisites of compliance. The fundamental benefit of certification and compliance is that it provides the confidence that there is no omission in any element of risk assessment; and that the industry security standard requirements are observed [30]. Therefore, saving the organisation from the security incidents, corporate reputation damages and penalties from the industry regulators, should a security breach occur [15]. It is therefore interesting to understand in a regional context, how organisation compliance influences security behaviour changes in employees and the threat landscape at large. Hence, the first motivation for this study is to explore the adequacy of compliance-based security in banking organisations, which also helped form the first research question discussed in section 1.4 of this thesis.

1.3.2 Malicious Insider Threats

Malicious insiders present a unique form of security challenge for organisations, given that insiders often have privileged access to critical assets; that make them the most serious security threat [23]. Insiders also constitute the most expensive form of a security breach, and the trend is set to increase significantly, despite organisations and government institutions' efforts on security tools and policy enforcement. [31].

In banking and financial organisation, the complexity of the operating environment and business processes is tied to critical information assets such that when adversaries carry out attacks, the effects often have colossal impacts on the organisation in terms of the loss of time, capital, human resources, reputation and competitive advantage [32]. Therefore, banks are under constant pressure to ramp up security; and banking organisations are more likely to upscale cybersecurity spending by a third, compared to non-financial organisations [33]. However, in situations where an employee already gains the trust of an organisation and has authorised access that bypasses most physical and electronic security measures, then the effectiveness of organisations' security effort is considerably influenced by insiders [34]. Thereby, suggesting that when it comes to deliberate and malicious activities, most organisations are ill-equipped to detect or prevent security violations from happening [35].

The motivation for this element of the current study is to assess how the factors that connect security protocols violation can be used to model and analyse a scenario for the prediction of malicious insider activities; as part of the holistic approach to security management. The insider problem discussed in the literature review chapter helps to form the second research question. The second research question is also developed as a direct consequence of the first research question, presented in section 1.4 of this report.

1.3.3 Resource Allocation for Information Security Investment

The priority of a security manager is to mitigate risk exposures that could undermine the organisational confidentiality, integrity and availability of

mission-critical systems. Although, there is evidence of increased likelihood of cyber threats for organisations [31], and in response, organisations are also likely to upscale security spending [33]. When an organisation operates on a small or medium scale, threat exposure is still imminent, but it is comparatively easier to maintain and assign resources for information security investment. However, as organisation scales up and the number of assets to be protected grows in the face of constrained IT budgets, there will be a point where a careful evaluation of information security investments will become apparent. However, an optimal level of resource allocation for security investment is often affected by intrinsically uncertain variables, leading to disparities in incentives and resource allocation decisions [36]. Top management in organisations may be unwilling to invest in security in the absence of incentives [37], while security managers may consider all risk facing targets deserving of proportionate security investment.

The motivation for this element of work is to explore how these disparities can be reduced within the context of information technology, and as part of a holistic security management. The research motivation and findings from the literature review also help form the third research question discussed in section 1.4 of this thesis.

1.4 Research Question

This thesis addressed three primary research questions as a way of contributing to the body of knowledge. The research questions are developed after an extensive literature review discussed in chapter two, the brief explanations presented in this section is to allow the reader to have a snapshot of the thesis narratives. The research questions are presented again with a detailed approach to how each question is addressed in chapter three (research design).

RQ1: “Is security by compliance adequate for the protection of organisation information assets?”

Most organisations adopt security standards for the protection of information systems, but when compliance is evaluated against security, the assumption is that compliance is substantially less demanding to quantify, but easier to justify in the event of a security breach. Therefore, compliance in isolation is a diversion from actual security. Is the assertion that compliance does not equate security true?

The reader may ask why this question is considered important, the response to it is that even though the problem domain that the research question stems from is not novel, the reality is that the problem is still valid and compliance gap still exists.

RQ2: “How can we profile malicious insiders by aggregating risk indicators from unrelated risk domains and safeguard security protocol violations?”

Malicious insider activities are difficult to lock down, given that insiders already reside behind the organisation firewall. Based on the review of insider threat to organisations, including data breach reports, individual personality traits and behavioural theories from academic literature; can we use the knowledge to suggest how insidious and hard to articulate form of insider security protocol violation can be addressed?

RQ3: “How can we address the issue of misaligned incentives and improve resource allocation decisions for cybersecurity investments?”

The challenges of resource allocation for the protection of organisation cybersecurity initiative is underpinned by the uncertainty in the budgeting process and the ability to forecast with any accuracy, the impact of a breach. Therefore, security resource allocation process is subjective and appeals differently to the risk appetite of significant stakeholders. How can we reduce the disparities associated with the process of security breach-cost estimation and improve security resource allocation decisions?

1.5 Thesis structure

The rest of this thesis is divided into three broad categories under section one, two and three. A graphical illustration of the research flow is shown in Figure 1.1 to capture the research process. Section one presents the extended literature review for this work, which helps pave the way for the research questions addressed in this thesis. In chapter two, the literature review is carried out to identify various gaps in the literature, especially in the areas of compliance, insider threat and information security investment. The gaps in the literature help clarify and refine the initial research questions. The research design and methodology are described in chapter three. It clarifies how research approaches, simulations and tools are applied to each of the research questions, and how the questions are addressed concerning the gaps in the literature review. The first research question is addressed in chapter 4 and chapter 5; the second research question is addressed in chapter 6, and chapter 7, the third and final research question is addressed in chapter 8. Section three covers the conclusions and suggestions for future work. The chronological order of the thesis structure and a brief description of each chapter is as follows:

Chapter 1. *Introduction*

This chapter introduces the research and presents a generic background leading to the problem statement and the motivation for this research.

Chapter 2. *Literature Review*

Chapter 2 presents the fundamentals and a brief overview of information security. It covers an extensive review of the literature on the three distinct areas of this work; standards and compliance, malicious insider threats and resource allocation for security investment. The review helps to identify the gaps in literature with respect to the domains of interest.

Chapter 3. *Research Design*

This chapter introduces the design adopted for this work by linking the research questions to the research methodology. It also describes how

primary and secondary data were obtained for quantitative analysis, simulation and modelling in this work.

Chapter 4. *Security by Compliance and The Implications for Banking Organisations*

This chapter answers the first research question based on a quantitative analysis of survey data obtained from banking organisations as a regional case study. It also covers how relevant theories help explain the quantitative analysis of survey data, to arrive at a conclusion on the implications of security by compliance in banking organisations.

Chapter 5. *Exploratory Study of Compliance-Based Information Security Management in Banking Organizations*

This chapter also contributes to answering the first research question by building on and extending the approach adopted in chapter 4, then using the Partial Least Squares Structural Equation Modelling (PLS-SEM) to explain our results. The compliance survey data obtained from banking organisations, the application of neutralization theory, and security scenario effects are combined to form security compliance hypotheses for this work. The chapter also helps to answer the question of why employees' violation of security protocols still occurs even though the organisation in which they work are compliant with industry security requirements.

Chapter 6. *System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis*

This chapter helps to address the second research question by presenting a system dynamics approach to the modelling of malicious insider activities. The model takes risk indicators from different domains to analyse the interplay between unrelated risk factors and show how they can increase the chance of cyber-security incidents in banking organisations.

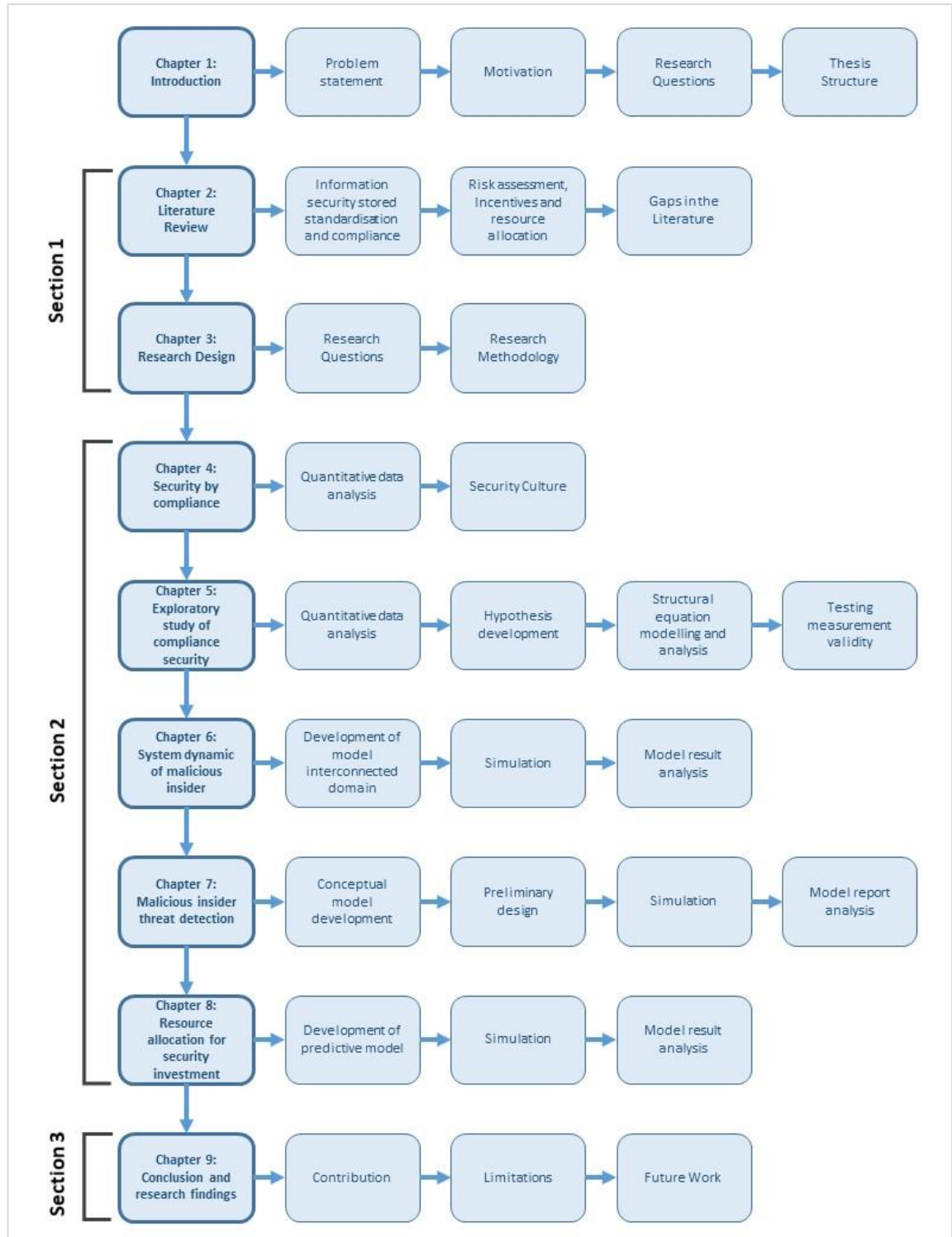


Figure 1.1 Thesis Structure

Chapter 7. *Malicious Insider Threat Detection: A Conceptual Model*

This chapter also addresses the second research question by presenting a conceptual model of malicious insider detection. The model aggregates the weighted values of different risk factors from unconnected domains and simulates the output using MATLAB. The result of the model can be used as part of the resources for managing organisation insider threat assessment. It can also be used to obtain insights about malicious insider activities, and draw inference about insider action during security breach investigations.

Chapter 8. *Towards Understanding the Incentives and Information Security Investment Decisions*

This chapter contributes to answering the third research question by presenting a Monte-Carlo Simulation model for resource allocation and security investment. In particular, it shows how using “ModelRisk”, a risk analysis tool and a three-point probabilistic estimate of the cost of data breach, can simplify cost estimation for complex asset classes in an organisation.

Chapter 9. *Research Findings and Future Work*

This chapter presents a summary of the key findings and contributions of this study to the body of knowledge and also touches on the areas of interest and suggestions for future work.

In this introductory chapter, the motivation for this work has been highlighted in three research areas of interest. It also shows how the problem statement links with the research motivation. The next chapter presents the extensive literature review for this work, leading up to the gaps in the literature and clarifies how the three research questions are developed and linked.

SECTION 1: INFORMATION SECURITY RISK MODELLING, STANDARDIZATION AND COMPLIANCE IN BANKING ORGANISATIONS

This section introduces the preliminary part of this research by presenting the extensive literature review of information security risk management. The literature review chapter specifically focuses on compliance, malicious insider problems and resource allocation for security investment. The breakdown of this section is as follows:

- Chapter 2. Literature Review
- Chapter 3. Research Design

2 LITERATURE REVIEW

“Securing a computer system has traditionally been a battle of wits: the penetrator tries to find the holes, and the designer tries to close them.”

- Gosser

This chapter presents the extensive literature review of this study. It is a particularly important aspect of this thesis as it introduces the reader to information security risk management in general; with a focus on standardisations and compliance, malicious insider threat modelling and simulations, and resource allocation for cybersecurity risk investment. This chapter starts with an introduction of the current threat landscape and concludes with the identification of gaps in the literature with respect to the three domains of interest.

2.1 Introduction

This thesis discusses information security in general with respect to systems, people and processes; as such, the term “information security” and “cybersecurity” are interchangeably used throughout the thesis. Although some academic materials highlight the difference in the two terms, suggesting that the two terms are not analogous [38]. Cybersecurity extends the boundaries of traditional information security by broadening the scope of attack vectors to include unknown participants and includes human targets in the scope of a potential victim of attacks; while information security is mainly about the protection of information resources and the element of the human factor in the security processes. In both cases, there are scenarios involving two different parties; one is motivated to exploit system vulnerabilities (adversaries), while the other is motivated to protect them (defenders).

As the interconnected and public-facing information systems increasingly get ubiquitous through the internet of things (IoT), so is the level of associated risks. In the information age, cybersecurity is considered to be vital to critical systems that interact with the real world in real-time scenarios [39],[40]; whereby the exploitation of those environments allows adversaries to raise the stakes significantly.

Adversaries ‘modus operandi’ varies a lot, depending on the level of attacks. At the enterprise level, through system hackers, there are adversaries that exploit systems for personal and financial gains or for business advantages. In most cases, the primary choice of weapon utilised to carry out malicious intent in the cyberspace is malware, through the exploitation of existing and emerging technologies [41]. Other forms of attack include different variants of ransomware attacks like the WannaCry, CryptoLocker, CryptoTear and Fusbo [42]. The WannaCry attack, in particular, locks up computers in demand of ransom which affected over 200,000 victims across government organisations, companies, hospitals and more than 150 universities [42]. At the State level, through cyber warfare, there are adversaries, primarily a nation-state and organised criminal gangs that are using cybersecurity vulnerabilities and cyber exploitations as a method to gain

access to networks, to potentially cause disruptions for strategic or military purposes. Classic example at this layer is the Stuxnet (computer worm) attack on the Iranian nuclear program computers, purportedly said to have been created by the USA [43]. There is also the case of Distributed Denial of Service (DDoS) attack on a number of Georgian government websites, commercial sites and media sites. The attacks were claimed to have been initiated by Russia [44]. While some organisation might not be the primary target of cyber warfare, their critical infrastructures like the economic system, financial institutions, stock exchange, water treatment plants, power grid and ATM systems, may provide a target of opportunity.

System hackers and the Nation States have the patience, the resources and the expertise to conduct tens of thousands of attacks on targeted systems. Therefore, system defenders need to embrace this new reality and begin to do things differently. The proliferation of systems and cyber-attacks is only going to increase, and there is no silver bullet to solve cybersecurity problems [45].

Security is a paramount concern for most organisations, but a secured environment cannot be solely based on technical tools. Therefore the human aspect of information security is increasingly considered to be as vital as a technical intervention for an overall security posture. However, the human dimensions in security efforts are often described as too trusting entities, such that even the most harden system can be breached via social engineering [9][45][46]. The anomalous human behaviour can be inherently complex, unpredictable and challenging to lockdown with a lot of cybersecurity instruments because the majority of the cyber defence tools are mostly focussed on IP addresses, ports and protocols of network security. The more technology integrates into our lives, so is the opportunity for the increase in system abuse. Technology is continuously evolving, but so are the associated security risks. Therefore the defence techniques to combat these threats must evolve as well through constant and innovative practices of cybersecurity awareness, investments and education [45].

The rest of the literature review chapter is structured as follows: Section 2.2 presents a critical review of the literature covering security standards and the current state of security by compliance. Section 2.3 covers a review of the theoretical perspective with respect to insider threats, modelling and simulation. Section 2.4 reviews the challenges associated with the allocation of resources for cybersecurity protection, touching on risk assessment and misaligned incentives. Section 2.5 highlight the gaps in the literature and also reinforces the significance of the research questions in this thesis, while section 2.6 summarises the chapter.

2.2 Information Security Standardization and Compliance

Standardization is the process of formulating technical consensus for parties sharing universal values in a given context. The purpose of standards development is to provide support for companies and consumer of products and services regarding product reliability, security and quality over a given period [47]. Usually, standards development arises through the efforts of experts from scientific institutions and companies that have string together a detailed description that characterises particular products or services. In the context of the information security management system (ISMS), organisations engage in ways to apply industry best practices to manage risks, and most of the best practices are the recommendation of international standards like the ISO/IEC 27001 and NIST SP 800-32 [30]. The rest of this section presents the framework for information security standards.

2.2.1 Framework for Information Security Standards

Managing information security through a code of practice enable organisations to certify their security processes through independent attestations, which supports and verifies the appropriateness and soundness of security measures for customers, clients and industry regulators. There are different variants of a framework for information security good practice, depending on the domain of application. However, international standards are universal.

The ISO/IEC 27K Series of Standard

ISO/IEC - The International Organization for Standardization (ISO) and the International Electrotechnical Committee (IEC) publishes the ISO 27K family of standards. It is a derivative of the original British Standard, which is an early draft of the guidelines on security management [30]. The origin of the ISO 27K family of standards can be traced back to the British Standard Institute BS 7799-1 IT Security techniques code of practice for information security management in 1995. There is also a complimentary part BS 7700-2, which explicitly provide guidelines for the certification of company processes [47]. The ISO harmonised the British Standard with other standards like the ISO 9001 in 2005 to develop the ISO/IEC 27001. The ISO 27000 provides the overview, introduction, explanation and terminology within the context of information security management systems. The certification standard ISO/IEC27001 (2005) forms the ISO27K standard foundation and requires that all controls, except on a firm ground of exclusion, be considered as part of an ISMS. Often regarded as the part two of the ISO/IEC 17799 (2005), the ISO/IEC27001 (2005) takes the form of recommendation, guidance and reference point for identifying controls needed for information systems [48]. The ISO/IEC 27002 comes with a catalogue of controls and code of practice for information security, though, ISO/IEC 27002 is currently under review, the review process is a regular occurrence every few years to preserve the relevance of the Standard in the face of dynamic and sophisticated information security threats. The ISO/IEC 27K family provides an area of comprehensive coverage that meets the risk management requirement of organisations in the area of business involving people, services, processes, information technology and physical assets [10]. The ISO/IEC Standard is robust enough to be adopted by both commercial and government organisations yet flexible to be used by small-scale organisations as well. The ISO/IEC 27001 Standard proposes 39 control objectives and 134 measures as part of the requirements for planning, implementation, operation and continuous monitoring. The control objectives are listed in Table 2.1, categorised under nine domains and comprehensively described in [11].

Domain	Control objectives
Security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
Organization of information security	To manage information security within the organisation. To maintain the security of the organisation's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
Asset management	To achieve and maintain appropriate protection of organisational assets. To ensure that information receives an appropriate level of protection.
Human resources security	To ensure that employees, contractors and third-party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. To ensure that all employees, contractors and third-party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organisational security policy in the course of their routine work, and to reduce the risk of human error. To ensure that employees, contractors and third-party users exit an organisation or change employment in an orderly manner.
Physical and environmental security	To prevent unauthorised physical access, damage and interference to organisation's premises and information. To prevent loss, damage, theft or compromise of assets and interruption to the organisation's activities.
Communications and operations management	To ensure the correct and secure operation of information processing facilities. To implement and maintain the appropriate level of information security and service delivery in line with third-party service delivery agreements. To protect the integrity of software and information. To maintain the integrity and availability of information and information processing facilities. To ensure the protection of information in networks and the protection of the supporting infrastructure. To prevent unauthorised disclosure, modification, removal, and destruction of assets. To maintain the security of information and software exchanged within an organisation and with external entities. To ensure the security of electronic commerce services, and their secure use. To detect unauthorised information processing activities.
Access control	To control access to information. To ensure authorised user access and to prevent unauthorised access to information systems. To prevent unauthorised user access, compromise or theft of information and information processing facilities. To prevent unauthorised access to networked services. To prevent unauthorised access to operating systems. To prevent unauthorised access to information held in application systems. To ensure information security when using mobile computing and teleworking facilities.
Information systems acquisition, development and maintenance	To ensure that security is an integral part of information systems. To prevent errors, loss, unauthorised modification or misuse of information in applications. To protect the confidentiality, authenticity or integrity of information by cryptographic means. To ensure the security of system files. To maintain the security of application system software and information. To reduce risks resulting from the exploitation of published technical vulnerabilities.
Information security incident management	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing the timely corrective action to be taken. To ensure a consistent and effective approach is applied to the management of information security incidents.
Business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
Compliance	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. To ensure compliance of systems with organisational security policies and standards. To maximise the effectiveness of and to minimise interference to/from the information systems audit process.

Table 2.1. ISO27001 Control Objectives (Disterer,2013)

Since 2006, The ISO/IES 27K family of standards has continued to register global growth rate, and according to the ISO survey report of 2016 [49], there is more than 20% increase in ISO/IEC 27001 certification. The United Kingdom currently ranks second and also accounts for about 10% of the global ISO/IEC 27001 certifications, only after Japan, as shown in **Error! Reference source not found.** of country rankings based on the overall ISO certificate issued.

Country	Certificates
Japan	8945
United Kingdom	3367
India	2902
China	2618
Germany	1338
Italy	1220
United States of America	1115
Taipei, Chinese (Taiwan)	1087
Spain	752
Netherlands	670

Table 2.2. Country rankings based on the overall ISO certificate issued (ISO, 2017)

In terms of figures, the total number of ISO/IEC 27001 certificates issued globally as of 2016, is just under 3500 as shown in Figure 2.1. The chart shows the consistent growth rate of certification from 2006 to 2016, and Japan is in the lead with 8,945 certifications. Japan plays a significant part in the global certification process because Japanese businesses are mandated to hold an ISO/IEC 27001 certificate [50]. The compliance requirement to the ISO/IEC 27001 certification is often domain specific as in the case of Nigeria, whereby ISO/IEC 27001 certification for all Nigerian banks and financial institutions were mandated by the CBN. Certification of ISMS that aligns with ISO/IEC 27001 not only project a positive image of security compliance to businesses but also offer a way to demonstrate the readiness to provide IT services in a secure environment.

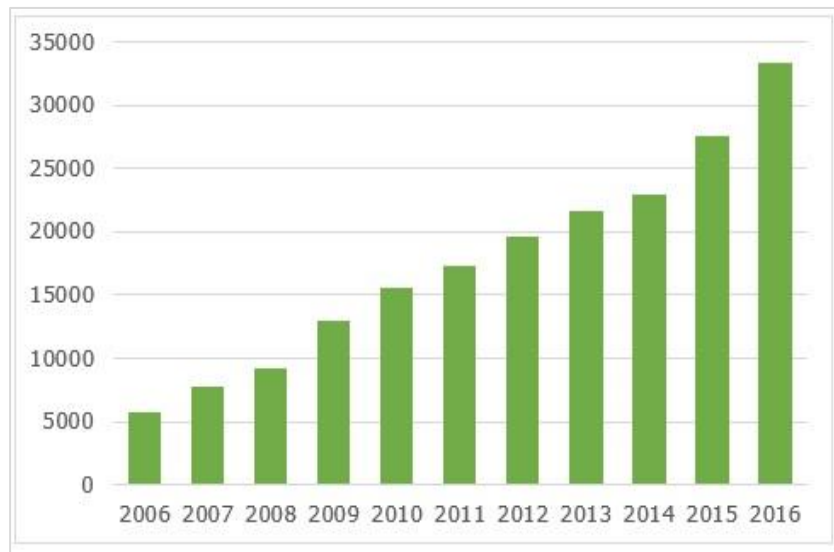


Figure 2.1. Number of ISO27001 certificates issued globally (Irwin, 2017)

Standards and Frameworks within the context of information systems are not limited to the ISO 27K suites alone. Although not extensively reviewed for this work, there are other security frameworks like the Risk Management Guide for Information Technology Systems '*The NIST special publication (SP) 800-37*', it is a US government standard developed by the National Institute of Standards & Technology (NIST) [51]. The Risk Management Guide is a qualitative and comprehensive risk assessment tool designed for skilled security analysts and technical experts to conduct risk management. NIST follows nine distinct steps of threat evaluation processes: 1) System Characterization 2) Threat Identification 3) Vulnerability Identification 4) Control Analysis 5) Likelihood Determination 6) Impact Analysis 7) Risk Determination 8) Control Recommendations and 9) Result Documentation [51]. Other frameworks include the Payment Card Industry Data Security Standard (PCI DSS) [52], the Health Insurance Portability and Accountability Act (HIPPA) [53], the Control Objectives for Information and Related Technologies (COBIT) [54] and the Gramm-Leach Bliley Act (GLBA) [55], just to mention a few.

2.2.2 The PCDA Compliance Model

The ISO/IEC27001 is an international standard for best practices for Information Security Management Systems (ISMS), which outline comprehensive requirements for safeguarding organisation information assets. It defines baseline requirements and controls for organisation risk assessment [56]. It is imperative that, for an organisation to meet its ISO/IEC 27001 requirements it must develop its Information Security Management Systems (ISMS) in line with a process model known as the Plan-Do-Check-Act (PCDA) model. The PCDA model ensures that the documentation, reinforcement and improvement of organisation best practices evolve with time [57]. The overall process covers three distinct stages as illustrated in Figure 2.2, where the model takes an input based on information security requirement and expectations; then produces an output of a managed information security. In-between the input and output, the PCDA model process goes through the development, maintenance and improvement cycle described as follows [19], [57]:

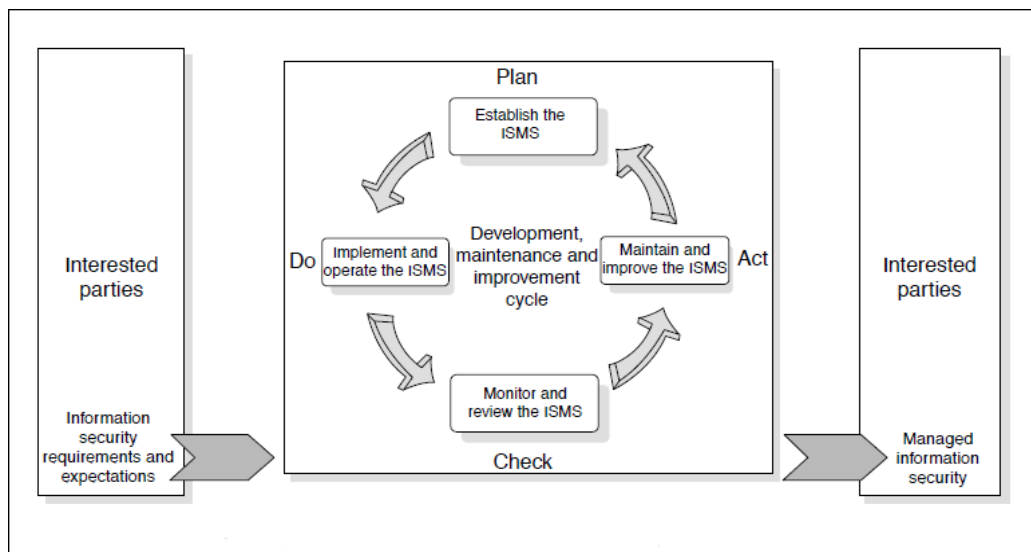


Figure 2.2. PCDA Model applied to ISMS processes (BSI, 2002)

The plan phase: This phase ensures that the scope and context of ISMS are established correctly and takes into account plans to identify security risks as well as appropriate treatment for each risk. Basically, the planning phase covers information security policy, scope of the ISMS, risk identification, assessment and treatment plan.

The Do Phase: This cycle implements and promotes selected controls for the management of information security risk, in line with all decisions, taken in the planning phase. This phase covers resource training and awareness, and risk treatment.

The check phase: This cycle is designed to check the effectiveness of controls and ensuring that they are working as expected; and if such controls are found to be inadequate either as a result of the change to the scope or assumption of security assessment, then necessary corrective actions are determined. The check phase covers routine checking, management review, ISMS audit and trend analysis.

The Act Phase: This phase is concerned with the regular improvement of the information collected during the check phase in order to maintain effective ISMS. The purpose of this phase is to take appropriate action based on the result of the check phase activities. In fact, any non-conformity issues, i.e. failure or absence to implement any of the requirements of ISMS is acted upon by taking corrective action in the Act Phase.

2.2.3 Information Security Cultural Framework

Organisation culture is described as the shared norms, values and attributes of an organisation that forms the basis for a sense of shared purpose, and sustain connections among people, processes and policies. It suggests that the management and governance of security are most effective when they integrate into the culture of organisational behaviour and actions [58].

In respect to risk culture, however, Information security culture is the ability to collectively harmonise the norms, values and attributes of individuals or groups within the organisation and operate subconsciously to identify, understand and act on current and future risks [59]. Organisation security culture is one of the well-researched areas of IS, and a number of studies recognised the need for creating security culture [60], [61]–[63] where employees have the attitude, skill and knowledge to support information security objectives.

Many discussions on the topic suggest how to make the culture of security consciousness come naturally to employees while performing their jobs. Information security culture should be all-encompassing, such that it compliments technical security measures put in place by organisations while remaining ubiquitous to the daily activities of employees [64]. There are significant linkages between effective security culture in organisations and the performance of information security governance as described in an empirical study [65]. The study suggests that while not focusing entirely on definitions that describes the manifestation of information security culture, the factors and attributes that conceptualises the idea of information security culture are equally important. There is a strong emphasis on security culture as a factor that encourages secure behaviour [9], it is described as the stage between the Gulf of evaluation (influencing factor) and the Gulf of execution (sustaining factor).

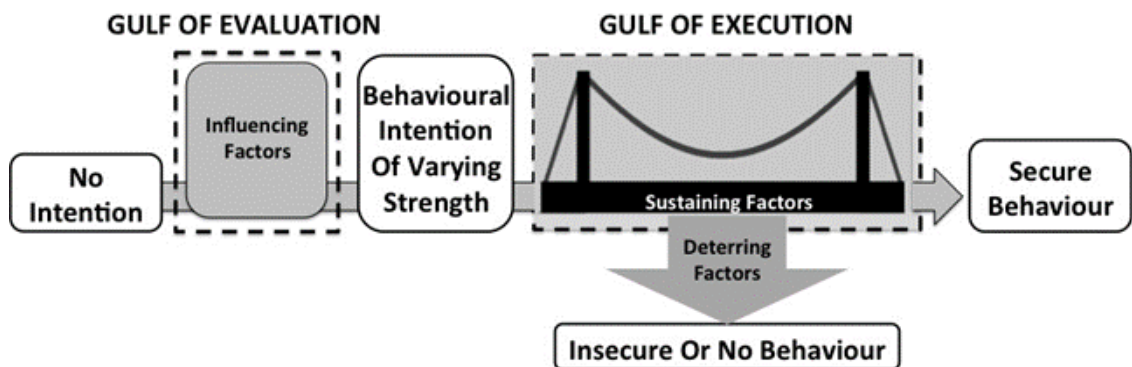


Figure 2.3. Antecedents of secure behaviour (Renaud, 2014)

The intention to violate security protocols transcends some progressive stages before the intention actually translates to either secure or insecure behaviour. Figure 2.3 shows the antecedent of secured behaviour, starting with the Gulf of Evaluation where an employee cultivates behavioural intention and evaluates some precautionary steps like awareness and response cost. Then there is the Gulf of Execution where the employee carries out the intention to violate protocol. However, the Gulf of execution also depends on two factors: 1) Deterrence factors like low level of expertise, response cost and the time lag

since the behavioural intention was formed. 2) Sustaining factors like security performances feedback, visible monitoring activities and social norms. Between these two Gulfs is the security culture, which helps to subconsciously modify and propel employees' intention from the Gulf of Evaluation, to secure behaviour at the Gulf of Execution. Organizational security culture entails that the assumptions, attitudes and perceptions that are accepted and encouraged must be maintained with the aim of protecting information assets so that attributes and custom of information security begin to emerge as the way things are done in an organisation [66]. Hence, a strong information security culture is vital for managing organisational information assets.

In addition, other studies described some reference points and comprehensive structures upon which organisations can cultivate an acceptable level of information security culture. For instance, the information security governance framework [48], shown in Figure 2.4 provides a starting point for the governance of information security. It explains how guidelines and control implementations can identify and address the technical, procedural and human components of information risks. The information security governance framework is derived from the integration of four different information security frameworks; ISO/IEC27001, PROTECT, Capability Maturity Model and Information Security Architecture (ISA) [48]. The framework comprises six key categories defined under strategic, managerial and operational; and technical domains. The categories that are most relevant to this work are discussed as follow:

- Leadership and Governance

This category comprises of the executive-level sponsor of policies and strategies for addressing the threats of information security. This category also covers the compilation and measurement of control effectiveness, in ensuring that organisation long-term security goals are met.

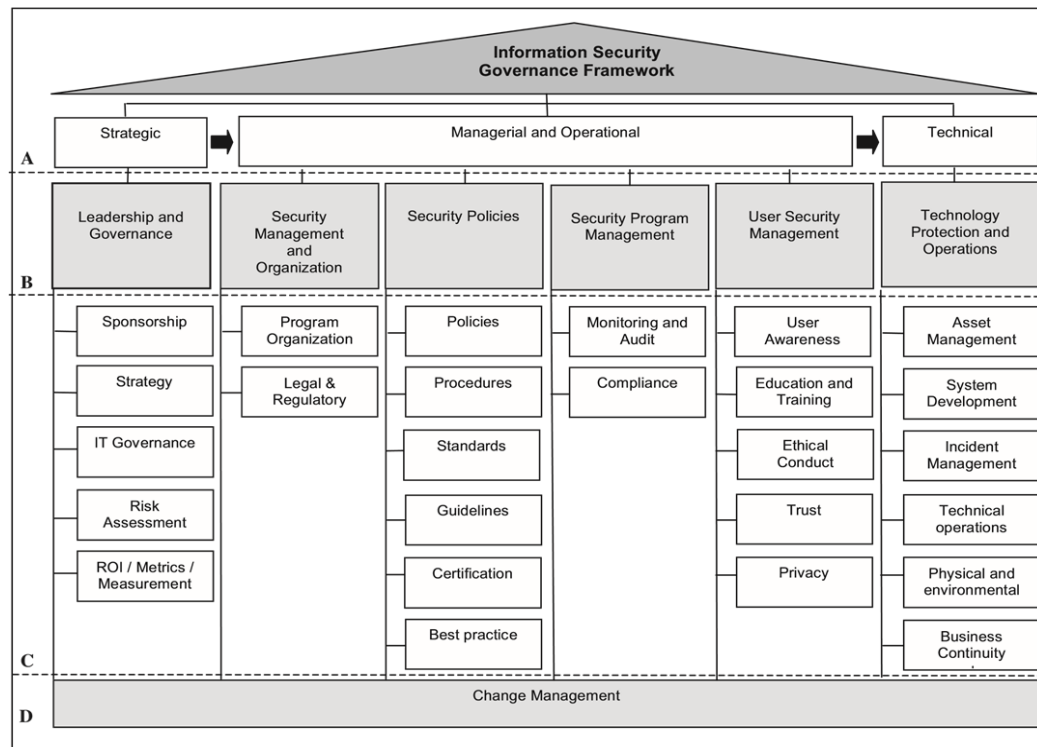


Figure 2.4. Information Security Governance Framework (Humphreys, 2008)

- **Security Management and Organisations**

This category addresses organisations legal and regulatory requirements for information security management. For instance, it is now a regulatory requirement for all Nigerian banks to be ISO/IEC 27001 certified. Also, the National Information Technology Development Agency (NITDA) guidelines on data protection draft (2013), requires that all federal agencies and private organisations that own, use or deploy information systems in Nigeria are covered by the guidelines [67]. Organisation information security design, composition and reporting structure are also addressed in this category.

- **Security Policies**

Security policies must be implemented through effective process and compliance while taking into account other components like legal and ethical considerations. Security policies are the overall organisation intention and direction as expressed by the management [68]. Policies provide a specific guideline for employee behaviour and procedures

when interacting with information systems. An example may include a point specific policy statement covering acceptable internet use.

- Security Program Management

This category involves auditing and compliance monitoring of both technical and human elements of security programs. It ensures that the management of policies, processes, procedures and controls are continuously monitored, for timely response to security breaches. Employee behaviour monitoring could include internet usage, while technology monitoring could be a network traffic monitoring.

- User Security Management

User security awareness, ethical conduct and trust are all addressed in this category. Ethical conduct is a vital component of security culture, it must be developed and communicated as part of a corporate code of conduct. For instance, organisation ethics may include unauthorised data alteration or disclosure. Security awareness program needs to be promoted and maintained throughout the organisation, and the management needs to find ways to integrate the element of mutual trust between all stakeholders.

- Technology Protection and Operations

This category involves physical and technical protective measures around information assets. As part of the implementation of the security governance framework, it must be ensured that the inclusion of appropriate technology controls is in asset management, technical operations, physical environments and business continuity. Continuous monitoring of technical controls is also critical to keep pace with rapid technology changes.

Habitual behaviour propagates, and it often requires concerted efforts to break the norm. If organisations want to project the habit of secure behaviour, perhaps a long-term goal that is in line with the direction of an organisational security culture is a better approach [9].

2.2.4 Information Security Risk Metrics

In order to conform to regulatory expectations, organisations approach risk treatment process through technical and human-centric dimensions to either mitigate or minimise the impact of threats. Most often, security investment decisions are the prerogative of the top management, who weighs the value of every investment against the organisation overall profit, regarding business returns. If security risk cannot be measured, it is hard to understand how it can be quantified to influence security investment decisions. Security metrics is defined as the values derived from the comparison of a predetermined baseline measurement taken over time, usually a product of data analysis derived from objective or subjective human interpretations [69]. However, measurement is the objective raw data generated from counting and provides a specific point-in-time view of situations. Security metrics allow organisations to measure its security initiatives against the backdrop of efficiency, effectiveness and return on investment (ROI). Metrics allows an organisation to take a bird view of its security awareness and provide insights regarding its information security program capabilities and regulatory compliance levels [70]. Security metrics is a vital decision-making tool regarding security measure impact to businesses, and it allows the questions of why the need for measurements, and what are the things to be measured? [71]. As shown in Figure 2.5, security metrics is an essential reference point in the organisational decision-making process that links organisation information security requirements with the need for measurements, so that resources can be optimised for the most critical security objectives.

In the context of ISMS, security metrics are concerned with system aspects that contribute to security and are somewhat more inclined towards qualitative measures that reflect the expertise and reasoned estimates of the evaluator. Often based on insight, intuition, subjectivity and induced ordering values that lacks the attributes of a useful metric [70]. When risk score is quantified on the ordering system of 1 = low, 2 = medium and 3 = high, which is often the case in an enterprise environment, results from specialised skilled risk assessors like a Penetration Tester are not always repeatable because they

heavily rely on the experience and knowledge of the evaluator. Ordinal numbers that grade relative score ratings in terms of low, medium and high are examples of the wrong application of metrics and does not measure anything [72]. In contrast, the right application of metrics is expressed as a cardinal number that can be counted and denotes a position of one thing with reference to another.

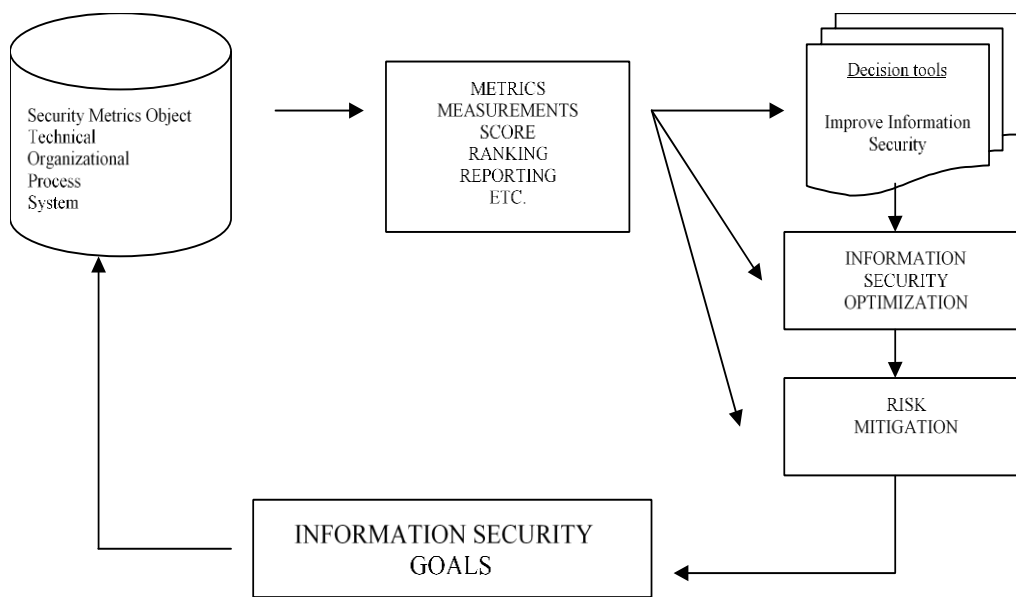


Figure 2.5. Security Metrics as management's decision-making tool (Vogel, 2017)

The difficulty involved to obtain right security metrics measurement is not to be underestimated [73], and enterprise-level security metrics, in particular, has been identified as one of the hard problems in the area of security research, from the perspective of INFOSEC Research Council [70]. Even, the overly exuberant use of ISO 27002/17799 and annual loss expectancy (ALE) scores are also considered to make the wrong metrics [72] as they do not guarantee consistency. The ISO 17799 for instance, focuses more on security control requirements enumeration and auditing rather than a comprehensive and balanced system of measurement. Hence, merely implementing security controls recommended in security frameworks does not necessarily equate to security measurement. Although, a correlation could be established that risk is significantly reduced by implementing a certain number of critical controls

of the ISO Standards, what reasoning could be put behind the selection of those critical controls rather than a different set of controls without any useful metrics? [72]. Correlation analysis is useful for establishing patterns, but if it fails to lead to the understanding of the dynamics that leads to the correlation, it is not much of use either.

2.2.5 Organisation Security Compliance Challenges

One of the ways that organisations manage ISMS is through the interventions of through security standards and compliance. Security standards like the ISO/IEC27000 series and the NIST SP 800 series address both technical and human aspects of information security by providing broad security framework and best practices applicable to different organisations requiring compliance. Actually, most organisation communicate their security capabilities through certification, as evidence of compliance with these standards [30]. The first challenge of information security management in organisations is the balance of incentives for the optimal mitigation of cybersecurity risks. Cybersecurity economic model suggests that depending on a combination of incentives, organisation policymakers may eventually stop investing in risk assessment and only focus on compliance-based security, which could lead to unintended consequences [74].

In addition, Standards don't quite often evolve as fast as technology and adversary technical expertise, but the most significant limitation to compliance-based security is the human factor. Research suggests that the human element is the dominant uncertainty variable of security [9], [75], as humans have the independent choice to uphold compliant behaviour intentions [76]. Security auditors and management may combine efforts to develop useable security policies, but employee compliance with policies cannot be guaranteed. In a publicly reported 2014 cyber heist [77], [78], a Nigerian bank lost £23.5m through an insider operating with rogue third-party contractors. Incidentally, the bank has been certified ISO/IEC 27001 compliant, in line with the regulatory requirement of the CBN.

Furthermore, some organisations apply deterrence measures to enforce policy compliance, but studies [79], [80] based on the deterrent theory suggested that employees' motivation differs across organisations. Hence, deterrent measures that work with one organisation may not necessarily fit into another. Deterrence also implies rational behaviour and even standards like ISO/IEC27001, COBIT and NIST draw on the principle of General Deterrence Theory [81], where rational users of information assets are expected to fit within a certain frame of reference. Although standardisation and regulatory demands play an essential part in attracting budgets and attention of C-level executives in the areas of information security, there are increasing challenges to balance real information security threats with compliance requirements [82]. Compliance security often leads to a heightened false sense of security and vulnerability perception.

Security standards and written policies assume sound rationale of users that interact with information assets. Humans are not programmable machines and often behave in manners that are entirely out of the norm [83]. There are many studies on why it is challenging to enforce compliance in humans. Consider technical security for organisations; it is difficult to audit human behaviour in the same way that technical auditing tools work [60], [84], because irrational behaviour borders on frustration, anger or despair propelled by lack of job satisfaction, vendetta, financial and personal problems [81]. Log files may capture and report unauthorised insider activities, but the insider behaviour and motives are not necessarily captured. Therefore, technical security audits verify the consequences of behaviour but not the actual behaviour itself.

There is a thin line between security and productivity [85], while compliance processes are aimed at hardening organisations security defence, sometimes, how standards are interpreted can contribute to porous security postures. If employees consider guidelines to be challenging to interpret or irrelevant to a business unit, it can easily give ground to non-compliance by way of accidental or deliberate introduction of threats to the environment [86]. It has been suggested that users often fail to adhere to policy

requirements because it is burdensome and there is no rational justification to comply from users' economic perspective; especially if the benefit is mainly speculative, or the consequence is of little or no harm to the users [87]. Some employees often felt compelled to opt for productivity at the expense of security or compliance, especially when additional steps are required to complete a task. In a survey of more than 500 professionals, over 60% admitted to using personal accounts to store and disseminate sensitive organisation data [88], because they felt that consumer options like free cloud storage accounts are more intuitive and easier to use than approved technology that sits within policy guidelines. The policy is an essential aspect of security, but it is only as effective as the technology and people backing it.

Apart from technical risk factors, the most significant threat to IS, leveraged through malicious and unintentional security protocol violation, is the human security behaviour [89]. There have been suggestions for more empirical research to link employee non-compliance with psychosocial factors and behavioural theories [90], in the attempts to explain the reason why employees fail to comply with regulations relating to cybercrimes. In today's fast-paced threat environments, the fundamental question is that, if organisations meet compliance requirements, does it actually translate to security?

2.3 Insider Threats: Theoretical, Behavioural, Modelling and Simulation Perspectives

This section introduces the insider threat challenges in the cybersecurity domain explained by theories that rationalise security behaviour. Organisations continuously face the challenges of insider threat on different fronts from data leakage to outright circumvention of critical information resources. The struggle for security experts to mitigate these threats is increasingly difficult as well, partly due to the proliferation and free availability of malicious tools as well as the anonymity these tools can provide for the adversaries [14]. Although, by default, decision makers in most organisations are more focussed on external attackers and business

continuity, in reality, the most expensive form of a security breach and highest business impacts are ascribed to malicious insider activities [23] [91]. Many kinds of literature agree that insiders are responsible for system exploits more than the failure of technical and procedural measures [7][8].

Insider problems are also widely documented in security reports. For instance, based on the U.S Secret Service and Verizon reports of confirmed security breach cases in 2009 alone, insiders are responsible for 46% of data breaches, of which 90% were malicious and deliberate acts [24]. Trusted users' elevated access to information utility is a primary concern when addressing the problems of insider threat, given that these users already sits behind organisations firewall.

2.3.1 Threat Agents

A threat agent is any person or entity that maliciously or accidentally initiate an attack to exploit system vulnerabilities. Threat agents are classified based on the access mode of internal and external threats. Threat agents are often considered malicious employees, but they do come in different variants, methods and objectives [92]. In general, abusive users of information systems that undermine the confidentiality, integrity and availability of organisations resources could have an internal or external affiliation with the organisation. Threat agents could manifest in the form of external attackers like vandals and data miners who operate for financial motives, competitors who operate for business advantage reasons, hacktivists who hacks into organisations for moral reasons or former employees who still harbour serious grudges [93].

Insider threat agents are mainly in an advantageous position based on the familiarisation with an organisation's security terrain, architecture and weakest points. Malicious insiders whose actions always put the organization's resources, processes and data under threat represents a serious breach of trust to organisations [94]. Insiders misuse of information systems mostly centres around destroying, modifying and stealing corporate data [26], and some of these illicit acts are carried out through technical capabilities. A study [95] of 36 illicit cyber activities in the government sector suggests that

24% of incidents are due to unauthorised privilege users, of which 11% involves the installation of backdoors. Similarly, in a case study of 52 cyber incidents [96], it is shown that 57% are detected through system irregularities of which 73% involves remote access logs and 57% involves unauthorised file access logs.

It is considered that malicious insiders require three distinct elements to violate security policies; motive, opportunity and capability. Motivation comes from internalising drivers like disgruntles, while the opportunity and capability are usually linked with the platform offered to those employees to perform their roles, like privilege access and training. Likewise, opportunity and capability could be attained secretly to circumvent organisation security as long as the motivation is present [97]. In terms of opportunity, however, security violations often occur as a result of negligence, carelessness or recklessness which are by no way malicious but accidental, while employees are trying to perform their job functions [98]. However, within the context of this work, malicious and accidental security protocol violations are all considered under the broad categorisation of the insider threat. Also, by definition, the meaning of insiders may be stretched to include affiliations like families, friends, spouses and client of insiders [98], but the definition and scope of an insider within the context of this research are limited to employees working in an organisation.

2.3.2 Threat Vectors

Information security threat vectors are the attack surfaces that an adversary can utilise to get past organisation defences, to infiltrate and propagate the network. As the threat vector increases so are the potentials for exploits. A single threat vector may contain multiple vulnerabilities, and the combination of these vulnerabilities is referred to as the attack surface [45]. The opportunities for cybercrime have exploded exponentially with the estimated 46% of the world's population (3.4 billion users) having access to the internet [45]. In today's threat landscape, the level of sophistication of hackers is growing, and the attack methodologies available to these hackers are also

becoming quite vast [99]. There are variations in the attack vectors by which industries are compromised as shown in Figure 2.6, with privilege misuse mostly notable in administrative, healthcare and mining industries [45].

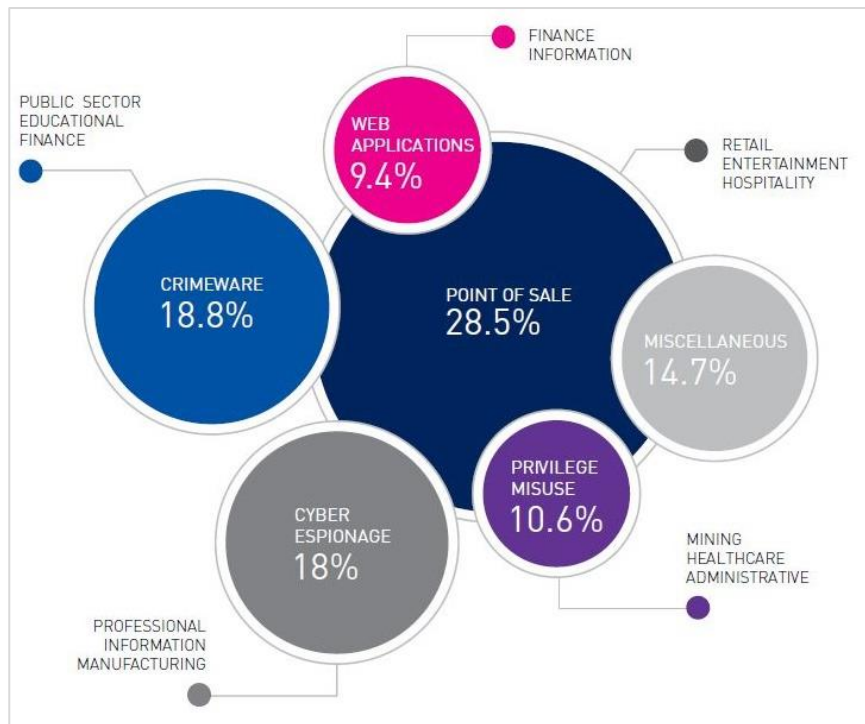


Figure 2.6. Threat vector by industry (Clive, 2016)

The ease of proliferation of today's data-laden environment has turned 'hacking' into a highly specialised profession with different layers of involvement. At the primary layer are hackers who are only interested in zero-day vulnerability discoveries and software exploits. Then, there is the second layer where a specialised group of professionals often buys the discoveries and run the packaged exploits through botnets. At the last layer are the individuals that flood the dark marketplace to rent botnets with the aim of gaining unauthorised access to other networks and computer systems [45]. Some of the routes that can be employed by hackers to proliferate network defences are briefly described as follows [45], [93]:

- **User (Social Engineering, Insider Privilege):** This type of attack may take years to develop, and it could even take longer to detect. It is the misuse of privileged access for malicious use of organisation resources. This attack could be initiated by an external entity that utilises social

engineering to obtain compromised credentials or an insider that is already residing behind organisation defence perimeters.

- **Network Perimeter (DDoS):** This type of attack mainly targets the availability and security of organisations resources, the underlying idea is to overwhelm network systems and applications by flooding it with service requests. Ultimately organisation resources like the email server may become temporarily unavailable or shut down entirely in some cases.
- **Web Applications (SQL Injection):** This category of attack is often carried out through botnets by injecting malicious codes or setting up phishing within application databases to steal personal information.
- **Crimeware and Ransomware:** These are considered one of the biggest cybersecurity threats today. They are mostly bots designed to automate the theft of proprietary information and personal entities. They can also spread viruses, spyware, worms and trojan horse.
- **Session Hijacking (Man-in-the-middle Attacks):** The session established between a computer and a remote server for the exchange of secure information can sometimes be intercepted by a third party pretending to either be the computer posting a request or the server posting a response. An attacker posing as a valid party in a session captures the session ID established between two parties and hijack a session to access unauthorised information on the server.
- **Cyber Espionage, Cyber warfare and State Affiliation:** This is mostly a form of organised cybercrime that targets nation states, public sectors, corporations and manufacturing industries. The same proliferation tactics of hacking, phishing and malware are deployed to seek similar outcome as hackers, except that these attacks are targeted, specific and extremely persistent. The proliferation of the cyberspace is sometimes from propaganda perspectives, to cause fear and discord, undermine economic confidence, and to disrupt and destroy strategic infrastructures.

- **Payment Card Skimmers and POS Intrusion:** This type of attacks mostly involve tactics like keylogging and RAM scrapping to access financial information data on credit cards, card skimming gas pumps and ATMs. The retail and food services industries are often the victims of these attacks.

This is not an exhaustive list by any stretch of the imagination, but the threat vectors are a few elements that seem to be common with almost every major security breach that happens today.

2.3.3 Insiders' Theoretical Frame of Reference

There has been a considerable number of studies in different fields like criminology, economics and social studies, that suggests that there is a strong link between individual's self-control, rationality, disposition and situational factors and the intention to violate information security policy [25], [100]–[102]. In the context of information security, the ability to predict human behaviours with precision is challenging, that is why there has been a plethora of independent studies on human behaviour and motivation, leading to theories in the field of psychology management and economics.

Starting with the Protective Motivation Theory (PMT), which is based on the natural predisposition for humans to protect themselves [103], suggests that when individuals perceive severe threats with a high degree of threat susceptibility, the natural reaction is to adopt the appropriate response to that threat as long as there is sufficient reason for self-efficacy. Therefore, self-efficacy strongly influences how individuals react to perceived threats or sanctions of security protocol violations [104].

The Theory of Planned Behaviours (TPB) suggests that human expresses certain cues in advance of security protocol violations [105] and that a person's perceived expectations, subjective norms and attitude perception towards crime are vital indicators of behavioural intention [106]. TPB suggests that human is fundamentally steered by three different types of beliefs [107]: The behavioural belief which is an individual expectation and evaluation of an outcome given an event. A normative belief which is the

willingness of an individual to comply with an expectation in respect to the expectation of others about the same event; and a control belief which is the individual intention facilitated by external factors. Therefore, motivation, environment and opportunity are linked to individual behaviour. Studies that explored the theory of planned behaviour [108], [109], also suggests that compliant behaviour can be attained through training and awareness programs. However, training is not sufficient to enforce compliance, despite the number of resources that organisations disburse to address security awareness gaps through training [9].

In the aim to enforce compliance, some organisations often introduce motivation elements of reward and punishment as a form of deterrence, so that employees can be discouraged from violating cybersecurity protocols. The argument on Deterrence Theory (DT) is that if an individual has the perception of severity and sanction for a particular behaviour, e.g. policy violation, then that individual may be dissuaded from engaging in such behaviour [110]. However, applying deterrence through reward and punishment does not always have the desired effect, as inferred by security practitioners and scholars in the field of social sciences [111]. This is because deterrence is subject to individual's rationality and relative morality.

In addition, studies [22] also shown that deterrence draws on the principle of rational behaviour, and information security standards like ISO/IEC27001 is also based on the assumption that people fit within a certain rational frame of reference. Therefore, contrary to logical assumption, deterrence measures often yield negative consequences, given that motivation that drives security consciousness differs across organisations [112], [113]. Instead, taking proactive steps to lower the perceived benefits of security violation and applying a high level of pre-employment screening for sensitive positions are the two directions for effective management.

In terms of the Neutralization Theory, it is a very relevant theory in the field of criminology. It describes the techniques adopted by individuals to justify deviant behaviour that violates expected norms and beliefs [114]. In the

context of information security, an individual may pre-emptively seek ways to promote episodically and neutralise guilts associated with security policy violations, through neutralisation techniques like denial of responsibility or denial of the victim. This is an essential element of human behaviour that influences the intention to violate organisation policy [115] because neutralisation techniques can be used to rationalise behaviour and to convince others why certain wrong action is justifiable.

Regarding human Personality traits, some studies suggest that individual Personality may be a critical indicator of what influences cybersecurity compliance [116]. Factors promoting the compliance or non-compliance outlook of an individual within an organisation could be unravelled through the understanding of a subject's psychological profiles [104]. According to the Big-5 personality dimensions measured by the NEO PI-R [117], the personality traits of openness, conscientiousness, extroverted, agreeable and Neuroticism (OCEAN) as shown in Table 2.3, can determine individual's behaviour.

Neuroticism	Extraversion	Openness to Experience	Agreeableness	Conscientiousness
Anxiety	Warmth	Fantasy	Trust	Competence
Hostility	Gregariousness	Aesthetics	Straightforwardness	Order
Depression	Assertiveness	Feelings	Altruism	Dutifulness
Self-consciousness	Activity	Actions	Compliance	Achievement-Striving
Impulsiveness	Excitement-Seeking	Ideas	Modesty	Self-Discipline
Vulnerability to Stress	to Positive Emotion	Values	Tendermindedness	Deliberation

Table 2.3. Personality dimensions measured by the NEO PI-R [47]

Also, the way individuals that are having any of the Big-5 personality types interact with situational factors is considered to be the strongest determinant of how they comply with security protocol [104]. Situational factors are external elements that can be influential as internal traits or motivation. In respect to information security, situational factors can interact with individuals' rational calculus to either comply with security policy or not [111], as defined in Table 2.4, based on the study of personality and compliance[104]. Individuals are different, so is their personalities which drive how they react to threats and sanctions.

Situational Factor	Definition
Self-Efficacy	Perceived confidence in the ability to comply with cybersecurity policy
Sanction Certainty	Perceived likelihood of being punished if the cybersecurity policy is violated
Sanction Severity	Perceived harshness of the punishment associated with violating cybersecurity policy
Threat Vulnerability	Perceived risk of something negative occurring if cybersecurity policy is violated
Threat Severity	Perceived seriousness of the risk associated with violating cybersecurity policy
Response Efficacy	Perceived effectiveness of cybersecurity policy
Response Cost	Perceived negative consequences associated with complying with cybersecurity policy
Realism	Perceived likelihood that a scenario such as the one presented could occur in the workplace

Table 2.4. Definition of situational factor (McBride, 2012)

2.3.4 Insiders' Behavioural Frame of Reference

Research linking cybersecurity compliance and human factor has expanded over the years, in an attempt to establish how individual differences shapes security policy compliance intentions. Security-related behaviour in organisation continues to generate research interest in the information security literature. Behavioural theories provide guidelines on how behaviour may manifest at different stages of an insider threat scenario by recognising observable 'concerning behaviour' that insider exhibits in advance of security exploits [24]. A study [118] shows that in 23 cases of insider threat in the banking and finance sector, 33% is due to personal problems that are unrelated to employment, like breakup and anxiety; 23% is due to revenge, 27% is due to debt, and 81% is due to financial gains. Also, based on a case study of 52 illicit cyber activities in the IT and Telecommunication sector [96], 33% of illicit activities are as a result of intolerant to criticism, 57% involves disgruntled employees, 47% is revealed through overt behaviour, and 58% involves direct communication of threat online.

There have been a variety of approaches to solving the malicious insider problem; some studies are based on behavioural analysis of a malicious insider to understand the key drivers of malevolent intentions. A review of some research done in an attempt to model insiders' threat behaviour in organisations is carried out, but this is by no means an exhaustive list. In terms of understanding the primary driver for malicious behaviour, some of the work in this area [95], [119]–[123] use decision algorithms to assess the predisposition to malicious behaviour by combining psychometric test scores data and real-time technical data obtained from users' information systems. Another literature describes malicious insider threats through a devised taxonomy of attributes; access, risk, knowledge, process and motivation, in order to analyse how each or a combination of these attributes stimulate malicious insiders' behaviour [124]. Bayesian network model [125] is applied to study the motivation and psychology of malicious insiders, while [126] evaluates the probability of insider threat detection through a conceptual model that connects real-world measurements and a hypothesis-tree, and [98] describes how technical assessment can be combined with information assets categorization and agents behaviour in order to mitigate insider threat problems through resilience, survivability and security.

In addition, research also shows that employees do not just carry out malicious acts randomly but show some signs of malicious behaviour well in advance of cyber attacks. In this light, some work emphasizes the importance of recognizing early signs of risky behaviour. For instance, [24], described a predictive modelling framework for automated support and detection of high-risk behavioural indicators that may help form risk mitigating decisions. Similarly, the work proposed by [127], evaluates the probability of IT misuse through the lens of multilevel hierarchical layers of threat components, the work provides an insight on how users' behaviour at the system level can be harnessed to predict computer misuse that originates from legitimate users. In terms of technical assessment, [128] shows how technical tools like the intrusion detection/prevention systems (IDS/IPS), and log analysis can be leveraged to uncover insider activities.

In terms of personality attributes, some research emphasises the link between personality traits and the tendency to become a malicious insider. For instance, [104] presents a personality evaluation approach that links cybersecurity protocol violation to the personality trait of a malicious insider, depending on deterrence, protection motivation or efficacy factors. Importantly too, some studies also suggested that people's personality can be revealed through the online social media platforms like the Facebook, Twitter and YouTube posts, from which personality types can be mapped to specific job roles, in order to mitigate insider threats [129], [130]. In particular, [120] reveals how it is possible to harvest publicly available information from YouTube video comments, that may identify personality traits through combined dictionary-based text classification and machine learning techniques. Similarly, [131] suggests that the personality trait of narcissism is a common characteristic of malicious insiders and that information shared in the public domain like Twitter can be utilized to establish predictive actions and deterrence measures against malicious insiders.

Although the approach adopted by some of the studies are criticised in [100], it is suggested that the data collection methods in most of the studies about human motivation and behaviour are plagued with common method biases, given that most of the behavioural studies are conducted through self-reporting and surveys. It is further argued that applying brain imaging technologies like electroencephalography (EEG) and functional Magnetic Resonance Imaging (fMRI) can increase the accuracy of data collection by observing the brain of research subjects as they contemplate decisions while interacting with information systems. It is assumed that this approach will allow researchers to establish neural correctness between brain processes and decision outcomes [100]. However, this approach is not within the scope of this study. Instead, relevant theories on human behaviour, motivations and personalities are explored within the context of information security management. This study extends the presumption that application of behavioural theories to human intentions and motivation to commit computer crimes are vital to the understanding of insider threats.

Finally, it is clear that personality drives behaviour, and behaviour influences how individuals interact with situational security factors. Previous studies have considered behavioural theories and technical solutions either in isolation or as a combined study. While recognising that insider threat constitutes a problem which already has damaging consequences for organisations, insider threats cannot always be detected or appropriately addressed with technical solutions alone [132], and there is a need for a framework that encompasses multiple risk indicators for a holistic and predictive threat detection [133], [134]. In this work, the behavioural, personality and technical risk indicators are combined and explored in a single study, to understand if there are inherent risks in certain personality types that can be expanded when aggregated with other risk factors from unrelated domains.

2.3.5 Modelling and Simulation

The challenge of enforcing cybersecurity controls against malicious insiders is to predict the presence of insider activities before it becomes a full-blown attack. One approach to overcoming these challenges is to model insider behaviour by aggregating some variables to reveal developing insider exploits. However, modelling human behaviour in a way that is entirely devoid of false positives is difficult [135]. Models are handy tools to replicate the real-world scenarios and reduce prediction error surfaces [3]. By moving away from forensic investigation whereby security analysts have to correlate and analyse an enormous amount of data, a predictive model offers the ability to infer underlying motivations and indicators for malicious exploits [24]. Unfortunately, the challenge around cyber data restriction limits research efforts in this area. It is increasingly difficult to obtain data regarding cyber-attacks either because organisations are not keen on sharing data breach information, defenders obtain data for specific purposes or attacker conceal their exploits [3]. However, data sets can be generated by simulation software, and some can be fabricated or obtained from security reports to test different aspects of a model [135].

Managing the insider problem is increasingly difficult and complex because organisations can concentrate on technical security features like intrusion detection systems (IDSs), firewalls and other authentication mechanisms, yet insiders may have the authorisation to bypass the checks to perform their job functions [3]. This is where behavioural analytics is useful for managing insider problems. The ability to simulate or model insider interaction with information system is vital to the analysis of insider threat root causes; also, for the evaluation of risk mitigation strategies in terms of people, process and technology [136]. However, the most difficult challenges in modelling insider threat are establishing precursors in terms of observable indicators [135], and verifiable data set.

Organisations are now embracing behaviour analytics solutions by focusing on the prerequisites for behavioural analytics, through policies. For instance, some organisations now modify policies to include the blockage of unwanted websites, remote access, two factor authentication and mobile device management, in order to create and store sequence of pattern for employees through role-based access control (RPAC), Mandatory Access Control (MAC) and Discretionary Access Control (DAC) Models [23]. This allows administrators to control and observe the way employees interact with organisation information assets. In a complex environment, where the distribution of uncertainties is not intuitive, it becomes even more important to have a system with the ability to define complex feedback from uncertain variables [137]. This is one of the important elements of the research space that this study seeks to address.

2.4 Risk Assessment, Incentives and Resource Allocation

There is a fundamental issue with the traditional method of risk calibration because some risk managers are not privy to the awareness of the full range of actions that can be implemented for risk reduction [5]. Information security risk analysis has always been viewed and evaluated from audit perspective whereby security auditors base their judgement on the use of checklists to verify that different elements of sound security ethics are in place and to

specify internal controls [138]. Central to organisation cybersecurity risk evaluation and investment decisions are C-level executives; who may not have a comprehensive understanding of their organisation security capabilities, information assets and threat vectors, yet decide the budget for security investment.

Most often, the C-level executives' understanding of risk tolerance is disproportional with the IS risk faced by their organisations and usually opt for compliance-based security solutions because it is easy to implement [139]. One specific shortfall of audit tools and checklist is that new threats and technological advancement catch up very quickly and checklist approach tend to become obsolete in no time [140], thereby requiring constant updates. Also, audit tools do not lead to advancement in scientific knowledge for information security design. The bottom-line is that, in the information security management realm, constructing tools that genuinely satisfy measurement theory is difficult [141], [142]. Even ISO Standard 27005 designed to help with the implementation of Information Security, does not recommend any specific risk assessment analysis method.

2.4.1 Appropriating Security Risks

Information Systems Risk Analysis (ISRA) has its root in decision theory, especially, the expected value (or utility theory). The expected value or utility of action may be thought of as having an underlying utility function, which represents choices in risky situations [143]. It can be calculated by defining a set of mutually exclusive and jointly exhaustive possible outcomes from a particular cause of action, then, multiplying the probability of each possible outcome by its utility. The expected Utility model is an empirically relevant model that could be applied to work out management preferences under a risky situation, especially where decision makers cannot tell which 'State of Event' will occur in a list of various possibilities and associated probabilities. For instance, given the function $U(.)$ which specifies how much utility is expected from a consumption; with probability π_1 , State1 happens, and c_1 is consumed, from which we get utility $U(c_1)$. Likewise, with probability π_2 ,

State2 happens, and c_2 is consumed, from which we get Utility $U(c_2)$. Hence, to consider the Utility that decision makers can get from a risky bundle (c_1, c_2) ; the expected Utility is specified as follows [144]:

$$U(c_1, c_2) = \pi_1 U(c_1) + \pi_2 U(c_2)$$

The expected Utility model is a better empirical approximation of the reality for choosing between risky bundles or situations as the case may be. It is about people's preferences with respect to the choices that have uncertain outcomes; where moral expectations contrast with mathematical expectations.

In contrast, the risk assessment methodology and formula that equates risk to the product of threats, vulnerability and impact of the threat, as proposed in [145], [146], as well as other relevant papers, could be described as unclear and mathematically over amplified.

$$\text{Risk} = \text{Threats (T)} \times \text{Vulnerability (V)} \times \text{Impact (I)}$$

The above formula is a popular and familiar format of Risk Matrix used as part of the risk assessment with applications across diverse fields like the project, climate, highway, cybersecurity, and terrorism risk management domains [147]. The risk matrix table shows a gradual response between the lower possibilities to the highest possibilities of threat and lowest impact to the highest impact of threat. The formula " $R = T \times V \times I$ " may violate the axioms of logical reasoning as it is quite unclear how to literally plug-in this concept into a mathematical formula. The evaluation of risk likelihood based on the probability of occurrence and impact is clogged with different shortcomings that are associated with subjective risk assessment; also, the theoretical basis for this approach is highly superficial [148]. Subjective probability estimates and can lead to overestimation of risk, a wrongful perception of the significant gap between lower probability and impact events as well as disproportionally viewing those with the higher risk. If there is no mathematical process or empirical data, mainly what it comes down to is inductive reasoning and trying to guess the odd. It becomes what may be considered as the developed methodology of chance and associated numerical values, which may lead to misrepresentation of the threat landscape [147].

2.4.2 Misaligned Incentives

The study of perverse incentive is a growing area of research in the information security management and cyber defence. A classic example of misaligned incentive as stated by one of the earlier proponents of research in this field is that banks in the UK typically spend more on cyber defence yet suffers more loss as a result of fraud compared to banks in the USA [149]. Misaligned incentives have been ascribed to the disparities in the way the body of proof is allocated in both jurisdictions. In the UK banking industry, the body of proof lies primarily with customers. Hence, banks may be less incentivised to manage risks associated with ATM Frauds compared to the banks in the USA where the body of proof lies with the banks. The US banks must either prove that a customer is trying to cheat or bear the cost of ATM card frauds, whereas, the UK banks generally get away with the claim that customers must be mistaken or lying because ATM system was secure [149]. Misaligned incentives also have a knock-on-effect on principal-agent relationships in many forms.

The problem of principal-agent relationship in respect to security investment decisions is not novel. Several reports touched on the recursive influence of perverse incentive on the overall security decisions in corporate organisations. In order to get security investment decisions correctly, the feeling of security needs to be aligned with the reality of security. Otherwise, the trade-off would always be wrong [27]. Also, the experience and background of independent monitors influence how responses and prioritisation are framed; this may lead to indirect 'manipulation' of principals perception and misinterpretation of the 'true state' of security [150]. For instance, Information Security risk assessor's background, experience and methodology are direct pointers to the risk score and the recommendation that determines management risk perception and security investment decisions. It is not surprising therefore that, independent evaluator's performance appraisals are subject to a significant amount of personal influence and subjective judgement [151]. When the interplay between risk perception and the reality of risk diverges, then risk calibration can be affected

in five major areas. Which in turn leads to poor investment decisions [27]: 1) Risk severity assessment 2) Risk probability assessment 3) Cost 4) Risk countermeasure, and 5) Security trade-off (between risk and costs).

At the enterprise level, incentive plays a significant role in the organisational reward system and how resources are allocated to defend enterprise information security. In the cybersecurity context, incentives are described as ‘the motives that system defenders have to do their jobs properly and also the motive that attackers have to defeat the defenders’ efforts’ [152]. Even defenders of systems that are motivated by the same goals, often get their incentive structures wrong. For instance, lack of symmetrised and effective incentive structure within an organisation may result in a clash of interest whereby the effort of system defenders, i.e. the Chief Information Security Officer (CISO)/employee is not aligned with the interest of system owners, i.e. CEO/Stakeholders [153]. This can lead to a distortion of risk perception and breach in security defence systems. The underlying problem in most information security policy is a misrepresentation of risk, informed by misaligned incentive [153]. A relevant analogy to elaborate this problem domain is a case of CISO of a business who is motivated to keep a system secure. There may be a performance metric associated with that, e.g. rewarding the CISO for maintaining the integrity of the system. However, business owners like the CEO and principal shareholders may be motivated by keeping low overhead costs, including IT budgets, to improve on annual profits and dividends. Perverse incentive presents a conflicting interest for security defenders even when working to achieving similar goals.

2.4.3 Allocating Resources for Security Investment

The budgetary allocation problems of information security investment have attracted contributions from several studies [154]–[157] in the attempt to propose justifiable optimum security investment decisions. Different approaches have been suggested, one of which is that the misaligned incentive scenarios can be presented as a game, where security defenders are modelled as participating agents in strategic interactions.

2.4.3.1 Game Theoretic Approach

Researchers have used game theory extensively, in the attempt to address conflict situations. In work involving data privacy and users attitude towards potential data breaches, a buyer-seller game-theoretical model of e-commerce transaction is proposed in [158]. The interaction between online buyers and sellers is treated as a game whereby players' maximising strategy depends on privacy policies, data usage and management. Similarly, [159] shows how user agents and cloud-based service providers like DropBox interacts in a trusting game concerning data privacy. Both works shed some lights on users' sceptical disposition towards potential online data privacy violation. Regarding the traditional risk assessment, where risk is computed as a product of threats and vulnerabilities, the authors of [160], suggested a game theoretical model whereby subjective estimation of threats and vulnerabilities are substituted with the result of a game. They demonstrated how a user and owner of an online bookstore could engage in the strategic game on data privacy challenges, where the user may be truthful or lie about his personal information, and the owner may protect or sell users personal information to a third party. The work showed how estimated payoff could be used to analyse risk rather than the subjective probability of events.

A one-period game model was suggested by [161] to address issues of security investment budgets. Optimum investment budget has always been a conflicting issue between security stakeholders regarding what is too little and what is too much when considered against the backdrop of security breaches and potential losses. It is shown that given two classes of security breach probability function, the optimum amount spent on information security is typically low and in the region of 37% less than expected loss from a security breach. Although the model did not take into account, issues of perverse incentives, and how one agent's decision affects the other. The authors of [162] took a pragmatic shift away from the traditional risk assessment method and presented a viable system model (VSM) for risk assessment in Industrial Control System (ICS). They proposed an approach whereby traditional asset-classification is replaced with VSM asset modelling in an ICS while taking into

accounts, the inter-relationship between those assets and (internal/external) environmental factors. The work provided new insight into risk assessment methodologies, especially at the asset classification stage. In a similar work, the authors of [163] proposed a model where a combination of VSM and game theory is used to manage cybersecurity risks in ICS. The approach was based on evaluating cyber components in an ICS with VSM modelling and then using the evaluation metric as input to a theoretical game between attacker and defender of an ICS. The work showed how strategies and payoff structures in the game could be used to propose a cost-effective protection solution. The study in [164] showed how system vulnerability could be reduced through security patches. A game-theoretic model was developed to study the strategic interaction between a vendor and a firm in balancing the costs and benefits of patch management.

2.4.3.2 Expected Utility Value Approach

Some studies also focus on the expected utility value of investment in order to determine the optimal resource allocation. For instance, the approach presented by [165] is based on the expected utility value suggesting that the level of investment for asset protection depends on the vulnerability of the asset and associated potential losses. The work further assumes that with increase in information security investment, the probability of security breach decreases but the marginal improvement in security also decreases with higher investment. Hence, risk-averse management may maximise the expected utility of a budget to determine the maximum amount to invest, which should not exceed the potential loss of breach. The approach presented [166], uses the term 'return on security investment' (ROSI), which is similar to the traditional accounting figure. The approach incorporates one-time costs and benefits of information security while it discards running costs and benefits as well as non-financial security measures, in order to support investment decisions.

$$\text{ROSI is calculated as: } \text{ROSI} = \frac{((\text{risk exposure} \times \text{risk mitigation}) - \text{solution costs})}{(\text{solution cost})}$$

where

$$\text{risk exposure} = \text{ALE} \times \text{ARO}$$

ALE denotes annual loss exposure while ARO denotes the annual rate of occurrence.

In work presented by [167], the information security investment decision is based on a balanced scorecard performance measuring system. This method, in its original context, evaluates organisation business performance from the angle of financial, customer, internal process and innovation. The authors extended and applied the balanced scorecard method in the context of information technology to support management decisions. The approach uses goal measurement to establish investment needs. Goal importance, e.g. server downtime reduction is weighted relative to other goals in order to set goal fulfilment minimum average degree. If an investment's average degree is considered to be above the threshold, then it is deemed economically viable. This approach considers all financial and non-financial mitigation measures.

2.4.3.3 Simulation Approach

There are other research efforts that also propose Monte-Carlo simulation for information security. For instance, [168] presents the Monte-Carlo simulation method for evaluating and communicating security investment benefits, and to understand technology choices in a financial manner. In [169], the authors describe probabilistic risk assessment to ICT systems, through scenario-based estimation of agent attack plan and risk impact. Then applies Monte-Carlo for detailed simulation of threat agents' behaviour to support assessment through statistical evaluation of risk. Similarly, [170] introduces Haruspex to simulate adaptive agents. The tool utilises a Monte-Carlo method to support evidence-based risk assessment and management, in furtherance of justifying appropriate countermeasures. The work in [171] presents a different approach to information security assessment based on the analytic hierarchy process (AHP) and Monte-Carlo simulation. In particular, the approach applies weight elements to the confidentiality, integrity and availability of information assets in order to improve the accuracy of results. The approach presented in

[172] addresses uncertainty elements in security risk assessment and visualisation. It combines system level process through risk analysis and probabilistic survivability assessment (RAPSA) and expert estimation through Monte Carlo, in order to quantify information risks as financial variables.

However, with respect to the related publications, this study uses the Monte-Carlo simulation approach to optimise resource allocation for security investment from a different perspective. This and other research space are discussed in the literature gap section

2.4.4 Some Prima on Interdependent Decisions and the Game Theory

Game theory offers a perfect tool for understanding human behaviour, incentives and motivation in a collaborative environment (that is, to either be honest and altruistic or dishonest and egoistic), where the result is a product of collective choices made by each participant. Game theory assumes that by default, rational players will make choices that maximise their payoffs, i.e. players will only be honest if it is more beneficial to do so. Otherwise, players will be dishonest, even though; it may be logical that participants will gain more from the alliance if all parties play the honest game. Game theory is an abstract framework-modelling tool for testing interdependent choices. It is a logical framework for understanding expected rational behaviour in human agents, but it does not solve the problem of how people behave. The empirical analysis is required to understand how human agents deal with problems of interdependent choices. Through experimental games in controlled environments, human agent's interdependent decisions can be observed and analysed to obtain empirical evidence that can help isolate the explanatory power of a variety of theories [173]. Theories are only logically correct, but we need to conduct some experiments to obtain empirical evidence to support or disprove theories.

2.4.4.1 Minimax Principle

Minimax principle is referred to as the cautious policy of avoiding the worst possible outcome in a strategic game. Following similar description in [173],

fundamental analysis of the minimax principle is shown as a payoff structure between player A and player B. In a finite 2-person zero-sum game, rectangular arrays of number always represent payoff matrix (a_{ij}) with row (m) and column (n) . The rule of the game is that if player 'A' chooses a strategy corresponding to row- i and player 'B' chooses a strategy corresponding to column- j , the number (a_{ij}) at the intersect represents the payoff gained or lost by either 'A' or 'B'. If complete information is assumed, both players know that their payoffs are inversely related. However, instead of selecting a pure strategy, a player may adopt a mixed strategy, thereby randomising his choice of row and column. For instance, a player may let his choice depend on an unbiased toss of coin.

A Mixed Strategy for player A is written as: $(x) = (x_1, \dots, x_m)$

A Mixed strategy for player B is written as: $(y) = (y_1, \dots, y_n)$

Assuming player 'A' uses a mixed strategy (x) , row- i will be chosen with probability (x_i) . If player 'B' uses mixed strategy (y) , column- j will be chosen with probability (y_j) , leading to a payoff of (a_{ij}) with probability $(x_i y_j)$, since both events are independent. Expected payoff is therefore the weighted average of all payoff (a_{ij}) occurring at probability $(x_i y_j)$.

This is written as $\sum = a_{ij} x_i y_j$

We know that the average payoff between player 'A' and player 'B' is inversely related, hence each player wants to maximise his payoff by minimising the other player's payoff. If either player knows in advance what strategy the other player will adopt each player will strive to use a corresponding strategy. Assuming that player, 'A' is aware that player 'B' will use a mixed strategy (y') , the strategy player 'A' will adopt would be such that it maximises his expected payoff against player 'B's (y') .

Hence, the expected payoff would be: $\sum_{(x)}^{Max} = a_{ij} x_i y'_j$

Likewise, if player 'A's strategy is known in advance to player 'B', the counter strategy for player 'B' would be such that it minimises player 'A's strategy.

Hence, player B's expected payoff would be: $\sum_{(y)}^{Min} = a_{ij} x'_i y_j$

In practice, these counter strategies may not be possible since both players do not have a pre-knowledge of each other's move. However, a player can maximise his payoff by assuming that any strategy (x) he plays will be minimised by the other player's counter strategy. In other to maximise expected payoff under this assumption, player 'A' will ensure that expected payoff is no less than: $\sum_{(x)}^{Max} \sum_{(y)}^{Min} = a_{ij}x_iy_j$

Likewise, with similar corresponding assumptions in mind, player B will ensure that expected payoff is no more than: $\sum_{(y)}^{Min} \sum_{(x)}^{Max} = a_{ij}x_iy_j$

If (a_{ij}) is any (m) by (n) payoff matrix,

$$\text{Then: } \sum_{(x)}^{Max} \sum_{(y)}^{Min} = a_{ij}x_iy_j = \sum_{(y)}^{Min} \sum_{(x)}^{Max} = a_{ij}x_iy_j$$

In the context of this work, the initial plan is to treat security investment decision as a multi-level game between different classes of players. Starting with a game between system adversaries that are continually seeking ways to attack organisation assets and system defenders that are continually seeking ways to mitigate the attacks, given limited resources. Then focus on sub-games between systems defenders (organisation stakeholders) that are incentivised differently to allocate budgets for security investment. In the sub-game, the idea is to apply a variant of the mixed-motive [2 x 2] experimental games like the Game of Leader or the Prisoner's Dilemma Game to explore how incentive influences cooperation and competition. Mixed-motive games are strictly non-zero-sum games. In economic and game theory, zero-sum games represent a situation where each participant's utility (gains) is the exact opposite of the other participant's utility (loss). By nature, zero-sum games are non-cooperative games where there exists a conflict of interest between participating agents. It is a game where the sum of payoffs for all players is zero whatever strategy each player chooses, in effect, what one player wins, the other player must lose [174]. Incentives to maximise payoff in zero-sum games is often predefined and non-negotiable, as such, zero-sum games would not have been an appropriate model for this work. Mixed-motive games, however, represent interesting psychological phenomena upon which precise

incentive models can be developed, i.e. risk tolerance and investment decision challenges.

As mentioned earlier, the initial plans to treat security investment decision as a multi-level game between different classes of players are dropped due to logistics constraint. The game theoretical element of this research is now being considered as part of the future work.

2.5 Gaps in the Literature

Following an extensive literature review, some gaps in the literature are identified that helps formulate the research questions in this thesis. Starting with the traditionally challenging cybersecurity problems, like compliance and malicious insider threats. Some literature suggests that additional researches are still needed in these problem domains [175]; and that a more holistic approach to security management is still very much needed [176].

The importance of standardisation is apparent, though it is uncertain how applying a blanket 'one-size-fits-all' approach to security as entrenched in standards can solve compliance problems [116]. There are questions on the practicality of Standards and Compliance alone when it comes to holistic security coverage for information systems. There is a gap between organisation compliance and organisation security since almost half of the organisation employees do not follow security policies either due to lack of awareness or as a result of incomplete or poorly defined policies [82]. The bottom line is that sometimes security breaches due to negligence errors are more prevalent than malicious acts.

In addition, studies reiterate the need to beware of information security stressor and work overload while enforcing compliance [177], therefore, a high impact compliance program that is delivered with minimum employee resistance is required. Also, works that explored the theory of planned behaviour [178], [179] suggested that training and awareness are the most significant factors that influence human behaviour and attitude towards information security. It was argued that attitude, perceived expectations and

subjective norms are the incentive components of behavioural intention. Hence, the change in employee attitude that is in line with corporate expectations can be addressed by information security awareness campaigns. Although some organisations put a concerted effort into training with the hope of addressing security awareness gaps, it is clear that training is not sufficient to ensure compliance and training is not the same as security culture [9]. What then can be done to ensure compliant behaviour? Can change be unforced? These questions represent the open space that this study tries to address.

Furthermore, a number of studies clearly recognises the importance of security culture [60], [61]–[63] to support organisation security objectives and compliance initiatives. However, steps on how to embed security into the culture of organisations are not addressed [180]. Similarly, the framework adopted for this study from [48], did not explicitly elaborate on how to embed security practices in organisation culture. How can compliance be integrated into organisation security culture? This is also one of the important gaps in the literature that this study strives to address by suggesting how this can be achieved based on the information security governance framework [48], discussed in the literature review. Later on, in this thesis, we explored a study based on security by compliance is undertaken while using Nigerian banks as a regional case study, to understand the implications of compliant security.

In terms of malicious insiders, the work in the domain of insider threat prediction is not a new area of research, but it has continued to generate interest among researchers. Previous studies indicate the inadequacy of attempts to address the human factor in cybersecurity despite the evidence that a malicious insider exhibits an observable ‘concerning behaviour’ in advance of the actual exploit [24]. The effort to curb insider problems continue to evolve, other studies on the malicious insider problems also suggested that an interconnected approach based on technical controls and behavioural methods can help security managers to curb the deviance of malicious employees [181]. In addition, relevant literature argues that detecting insider activities requires more than a single indicator, recommending the need for a framework that encompasses multiple risk indicators for holistic and

predictive threat detection [133], [134]. This study recognises the vital contribution of other models. However, it is believed, to the best of our knowledge, that previous studies have not considered the crucial element of personality trait along with behavioural and technical risks in a single study, in order to model the insider threat scenario. In this study, the personality dimension is included in the study of insider threat. If each individual's personality trait interacts differently with security scenario effects and also determines the susceptibility to violate security protocols [104]; it is, therefore, essential to include personality traits to the insider's threat landscape. This study considers a model of insider threat from different perspectives and domains that are naturally unconnected and then try to use some form of analytic approach to connect security risks from these domains; to showcase the activities of a malicious insider with presumably increasing accuracy.

Finally, to encapsulate the first two identified problems of compliance and malicious insiders. There is a need to consider how to allocate budgets for security investment as a single block while taking into account, the increasing number of assets and the risk of a security breach to those assets from the perspectives of organisation stakeholders [182]. However, with respect to the related publications, our work uses the Monte-Carlo simulation approach to optimise resource allocation for security investment from a different perspective. The work discussed in this thesis is based on a predictive modelling approach and offers a different dimension to information security resource allocation problems. This study applies Monte-Carlo simulation in the context of information technology to a single block optimal resource allocation at an organisational level. Information security management is an evolving security problem with different layers of complexities. All these complexities have made security more challenging for system defenders, and the purpose of this thesis is to evaluate the human aspect of information security and management against the backdrop of compliance, malicious insiders and security resource allocation problems. These identified gaps in the literature are addressed in chapter 4 to chapter 8 of this thesis.

2.6 Conclusion

A thorough review of academic literature is provided to aid an in-depth understanding of compliance issues relating to ISMS in organisations. Also, the human factor element of enterprise security is intensely reviewed while touching on relevant behavioural theories from other disciplines. In the literature review, the current challenges and research efforts in information security management with respect to compliance, malicious insider problems and the resource allocation problems for security investment are presented. This study looks at how to improve the gaps identified in the literature review and propose an improvement to holistic security management. In particular, this study looks at organisation compliance problems and the factors undermining compliance effectiveness. Then linking the findings to malicious insider problems and how insiders rationalise their behaviour to violate security protocol.

The topic of the insider threat is an elusive one for most organisations, such that it is often met with resistance or denial that insider threat is a very likely event with devastating consequences. A simple case of lousy action or judgment from a third party and privilege users present the same security concern as external adversaries, if not more. Also, it is apparent that even if insider actions are not necessarily malicious but inconsistent with organisations security policy and guidelines (e.g. clicking on links in phishing emails), that significantly places attackers at an advantage against system defenders and broadens risk exposure to organisation security. In the security game, ignorance is not an excuse for complacency. Dealing with unintentional or malicious insider threat comes down to organisation resilience. Security resilience entails the design of a network with the presumption that there will be a compromise and be able to mitigate that compromise in a timely fashion. When there is a security breach incidence, the quicker it is spotted and mitigated, the quicker damage can be controlled. Through architectural security choices, an organisation can increase its visibility towards a better resilience in the phase of increasing insider activities.

Organisations continue to invest in cyber resilience, for instance, VPNs and Firewalls are the two most prominent traditional security features that organisations use today, but they also present many weaknesses. The problem with firewalls, for instance, is limited operational fluidity, as they are static defence mechanism and controls deployed in dynamic environments. Firewalls do not automatically respond to infrastructural or environmental changes. Once firewalls are configured, they do not necessarily dynamically respond to infrastructural changes without administrators' interventions, or policy and rule changes. Firewalls are not specific to address granular user's access to resources instead it is focussed on large-scale networks by focussing on ports and IP addresses. However, real users are not devices and IP addresses, most importantly system adversaries do not always reside outside the security perimeter. VPNs and firewalls are single ingress-point border control devices and once authenticated, VPNs can access the whole network that is exposed to in many cases. Therefore, a better approach to security must be humancentric focused, where users' behaviour and personality traits are linked with how they interact with organisation resources, then, constantly monitored and dynamically evaluated against organisations overall security goal.

Finally, this study reviews how the interplay between risk management approaches and diverse incentives affects resource allocation decisions for security investment in organisations. In addition to investing in countermeasure capabilities to prevent losses and system failure as a consequence of cyber-attacks, organisations must budget for the right level of investment to mitigate those risks. However, because of the lack of an accurate measurement of the cost of security breach or impact of the attack, it is often difficult to estimate budget for risk mitigation initiatives; a problem space that is still valid and needs to be addressed. In the next chapter, the proposed research design is introduced, then each of the research questions is linked to the research methodology adopted for this work.

3 RESEARCH DESIGN

"It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it."
-Stephane Nappo

In this chapter, an in-depth approach and justification for the research design are presented. After identifying the literature gaps in chapter 2, this chapter shows how each of the research questions is formed and how they are linked to the research process. The research methodology, data collection methods and simulation steps that are followed to answer the research questions are also covered. For completeness and ease of understanding for the reader, this chapter features an overview schema of the high level and low-level research process.

3.1 Introduction

Research methods are predominantly applied to problems to find viable solutions that are testable and verifiable. Research is described as a systematic and unbiased approach to answering questions and support hypothesis through verifiable data with the aim of solving a problem [183]. Various research methods can be applied to different problems scenarios depending on how the research method fits with a long-term solution to the research problems. In this study, a mixed methodological approach is adopted. It is based on qualitative and quantitative analysis, leading to an explanatory and predictive output to answer the research questions and explain the findings of this research. Elements of theory, modelling and simulation are also applied to enhance the narratives of this work.

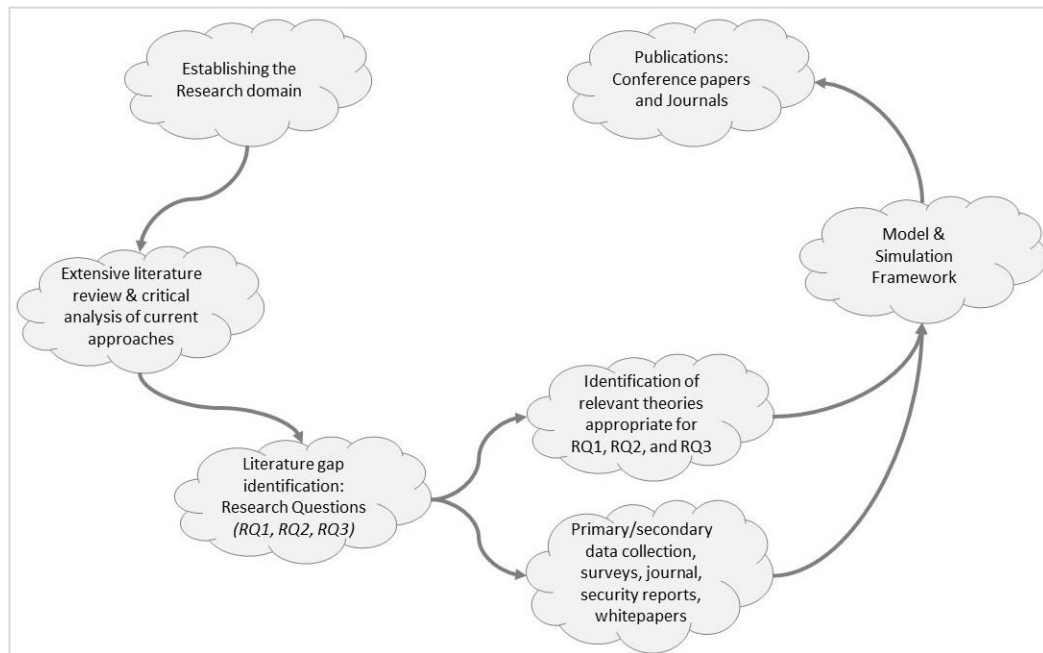


Figure 3.1. A high-level overview of the research process

The research design is structured, such that, each research question is framed based on gaps identified in the literature reviews, and the response to each question is addressed based on the best-fit research methodology. Figure 3.1 shows the high-level overview of the research process, starting with the establishment of the research domain. At the infancy stage of this work, an extensive literature review and critical analysis of the current approaches is

carried out. The output from the stage is covered in chapter 2, the literature review. Follow on from the literature review stage, gaps in the literature are identified, which leads to the three research questions in this thesis.

Two parallel methods for data collection were set for this research; the first one is based on primary and secondary data collection through surveys, academic articles, white papers and data breach reports. The second is based on the identification of appropriate theories which helps answer each research question. All the relevant theories are extensively covered in chapter 2. The output from this work is in the form of exploratory study results, simulation, conceptual modelling and measurement validation, parts of which have been published in journals and conference proceedings. In the next section, key elements underpinning each of the research questions and the steps taken to address them are presented.

3.2 Research question

In this section, each research question is presented followed by a brief description of the research focus, the relevance of each question to the overall research output and the steps taken to answer each question. The order of the formation of the research questions and how they link to the domain of study as shown in Figure 3.2. A low-level overview of the research process is also shown in Figure 3.3, demonstrating the phases of the research process and what the research output is in each phase.

RQ1: “Is security by compliance adequate for the protection of organisation information assets?”

Information security policies, guidelines and regulatory standards describe the security requirements expected of an organisation to protect its information assets. In some cases, these standards are industry-specific and obligatory; and in other cases, they are compulsory requirements enforced by the regulatory bodies for that industry. The banking and financial institutions are more vulnerable to cyber-attacks given that they present most public-

facing products and services, consequently, they are always faced with the challenges of managing security [45]. In recognition of this, some jurisdictions have enforced regulatory standards and compliance initiatives to combat cyber risk in financial institutions.

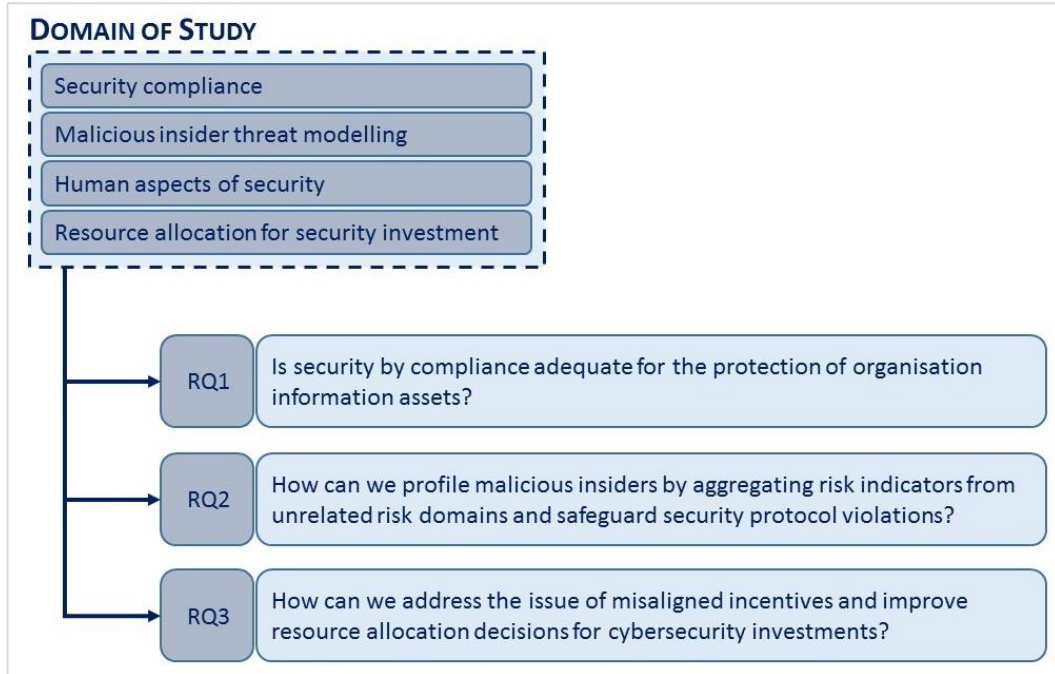


Figure 3.2. Research Questions

In the united states, the jurisdiction adoption is the National Institute of Standards and Technology (NIST) Cyber-security Framework (CSF). In the United Kingdom, the jurisdiction adoption is the Bank of England’s CBEST Framework, for the delivery of intelligence-led security tests; and in Hong Kong, it is the Cybersecurity Fortification Initiative by the Hong Kong Monetary Authority (HKMA) [184]. However, in Nigeria, the jurisdiction adoption is the ISO/IEC 27001 Standards mandated by the Central Bank of Nigeria (CBN) for all Nigerian Banks and Financial Institutions. In this study, we explored the Nigerian jurisdiction adoption of ISO/IEC 27001 Standards as a regional case study for security compliance in banking organisations.

The steps taken to answer the first research question are summarised as follows:

- Identify how Nigerian banks are certified for the ISO/IEC 27001 Standards as a compliance requirement of the apex bank CBN.

- Identify the effectiveness of the ISO/IEC 27001 Standards and compliance regarding the banks' overall security posture.
- Identify relevant behavioural theories that may undermine the effectiveness of security through compliance.
- Apply theories and develop a survey questionnaire for quantitative analysis to help draw an inference and generate descriptive results.
- Perform Partial Least Square Structural Equation Modelling (PLS-SEM) for validity testing.
- Result analysis and discussion.

Chapter 4 and 5 presents a detailed answer to research question 1, parts of the research output for this piece of work have been published in HAS2016 and WMSCI2017 conference proceedings as well as the JSCI2017 Journal.

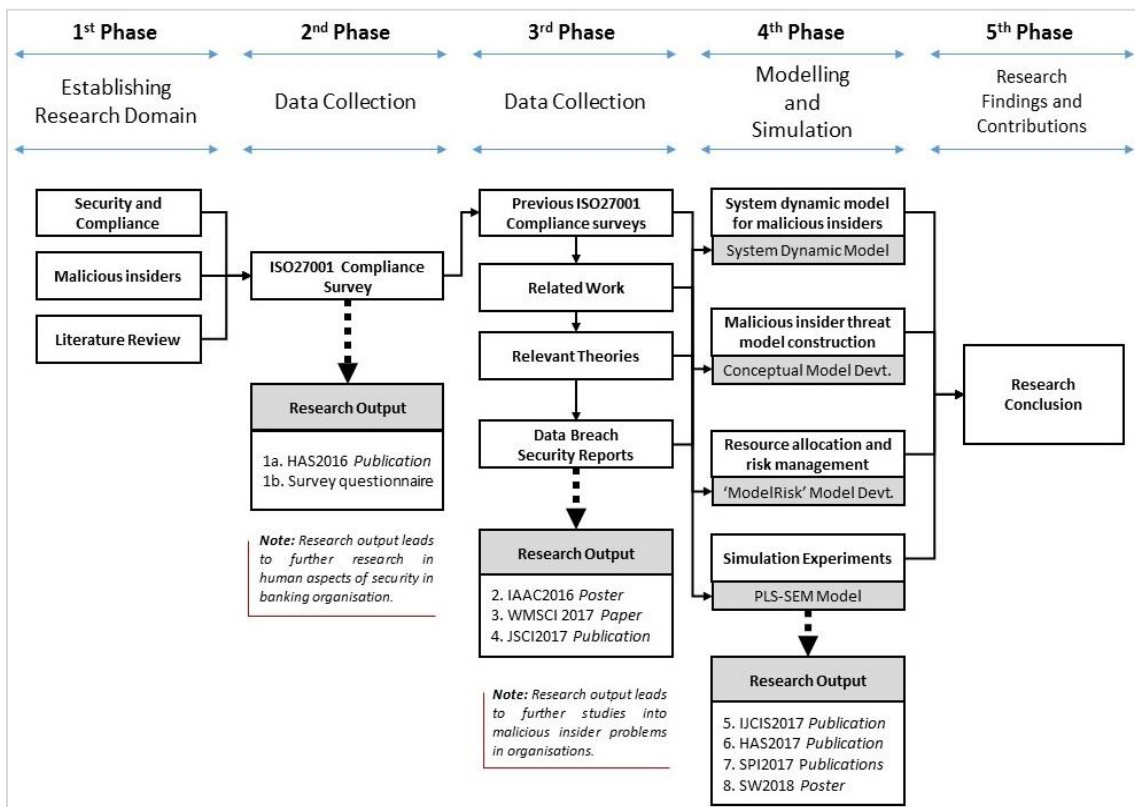


Figure 3.3. A low-level overview of the research process

RQ2: “How can we profile malicious insiders by aggregating risk indicators from unrelated risk domains and safeguard security protocol violations?”

Following the research question 1, it was established that security by compliance is a far-fetched approach regarding organisation security posture. In many cases, it is not the security policies or standards that is inadequate but because of the human element, which is the weakest link [9]. Human behaviour is an unpredictable variable in any security effort, and the insider problem continues to generate interest among researchers [3]. The second research question is to address the malicious insider problem by aggregating risks indicators from unconnected risk domains. The idea is based on the fact that insiders do not violate security protocols on a whim. Instead, they show in advance of attack some subtle behavioural patterns. Although, behavioural risk attributes may be nuance and appear to be unconnected with the intention to violate security protocol, especially when treated in isolation. However, when risk indicators are aggregated from other risk domains as well, this study assumes that the chances of positively profiling a malicious insider increases.

The steps taken to answer the second research question are summarised as follows:

- Identify relevant behavioural theories that provide guidelines on how human behaviours manifest at different stages of an insider threat scenarios.
- Identify literature that links human behaviour to the intention to violate security protocol.
- Identifies theories and literature that statistically links personality profile to the susceptibility to violate security protocols.
- Identify the frequency and pattern of a technical security breach from relevant literature, data logs and information security data-breach reports.

- Develop a System Dynamic Model that describes the dynamic relationship between an insider's behaviour, personality and the probability of a cyber security incident.
- Perform simulation analysis showing how the aggregation of risk variable from unconnected domains can indicate early signs of the intention to violate security protocol.
- Result analysis and discussion.

Chapter 6 and 7 present a detailed answer to research question 2, parts of the research output for this piece of work have been published in HAS2017 and SPI2017 conference proceedings.

RQ3: “How can we address the issue of misaligned incentives and improve resource allocation decisions for cybersecurity investments?”

After addressing the research question 1 and 2, our findings lead to research question 3 which is based on cybersecurity planning, resource allocation and decision support. Ultimately, organisations want to defend against security breaches and ensure compliance by its employees. Security incidents can be as a result of external attacks, malicious insiders or unintentional security violation [91], either way, the financial impact of cyber-attacks is often colossal, extremely damaging to business continuity and challenging to quantify [45]. More so, the decision process to allocate resources for cybersecurity investment is often difficult because of the diverse incentives and preferences over risks prioritisation between security managers, investors and C-level executives [153]. Security managers are interested in security-enhancing assets at the expense of cash flow; while C-level executives are interested in productive assets that guarantee a long-term profit. Although, cybersecurity is increasingly considered vital for managing organisations financial risk but how to measure high-impact security risks, plan for mitigation efforts or prioritise resource allocations is difficult, given limited security budget.

The steps taken to answer the third research question are summarised as follows:

- Identify relevant literature that links optimal resource allocation problem to the disparities in resource allocation decision.
- Develop a conceptual model of an enterprise as a case study for resource allocation decision support.
- Identify the verifiable historical cost of data breaches in organisations from security reports as parametric values for the conceptual enterprise model.
- Perform Monte Carlo simulation within the context of information security to show how to reduce the disparities in resource allocation decision.
- Result analysis and discussion.

Chapter 8 presents a detailed answer to research question 3, parts of the research output for this piece of work have been published in the IJCIS2017 Journal.

3.3 Research Methodology

The research methodology adopted for this work is based on the combination of qualitative and quantitative study as well as modelling/simulation-based approach. The appropriateness of these research approaches lies in the applicability of this study. Qualitative research is particularly appropriate for situations where a detailed understanding of the subject matter is required [185]; especially where the outcome of situations can be affected by the underlying perception of the participants. The outcome of the qualitative study is a product of quantified elements expressed regarding contextual implication. Quantitative research allows the presentation of a snapshot view of samples for generalisation purposes, especially where a standardise comparison is vital to the breath coverage of many people or events [186]. Also, the ability to apply statistical methods for validity testing, measurement and analysis improve the soundness of the approach regarding an objective

outlook. Modelling and simulation-based approach offer a platform for developing insights to model real-world scenarios [137]. Models are particularly useful where problems are complex, and real-life experimental solutions are impractical [187]. In the case of enterprise cybersecurity, where critical information assets cannot be subjected to real-life experiments or human behaviour which is difficult to predict; modelling and simulations are valuable platforms where the interplay of complex variables can be simulated in abstraction to explain the phenomenon that may be too costly to experience directly. This work combines elements of qualitative and quantitative research from which primary and secondary data were obtained as parametric variables for the research modelling and simulations.

3.3.1 Qualitative and Quantitative Research Approach

As described in section 3.3, a combination of qualitative and quantitative or what may be considered as a mixed methods research design is adopted for this work. This approach allows the exploration of a single research problem by integrating elements of both quantitative and qualitative methods, regarding data collation and analysis [188]. A qualitative approach investigates local knowledge and understanding of a given issue or people's expectations while a quantitative approach explores specific and clearly defined questions that examine the relationship between two events. Starting with a qualitative approach through semi-structured interviews of a small number of information security officers, some factors that may undermine employee compliance to information security protocols in banking organisations are identified, while using Nigerian banks as a regional case study. The interview approach has been considered to be useful to generate true feelings of respondent on contextual issues especially at the early stage of research [189]. The qualitative data obtained is used in the design of the survey questionnaire in order to generate quantitative data. In particular, through the information security survey questionnaire designed for employees of the banks, it is possible to establish an understanding of respondents' attitude to security policies by capturing survey responses to

“security culture statements” and *“security knowledge and awareness statements”*. Also, the quantitative data generated is used for model validity testing. There are significant advantages in adopting mixed model research as explained in literature because it broadens the range of data sources and methods of data collection; therefore, the quality of research outcome is considerably increased in terms of result validation, interpretation and context [185]. The following sub-section describes how data are collected from primary and secondary sources for this work.

3.3.1.1 Primary Data

Interview: The research interview is one of the most important qualitative research data collection methods [190]. Semi-structured interview questions are developed specifically for CISO of the participating banks (as a regional case study) in order to capture the depth and effectiveness of compliance with the ISO/IEC27001 Standardisation. Case studies are best chosen when the boundaries between phenomenon and context are blurred; and allows the exploration and understanding of complex issues particularly when a holistic, in-depth investigation is required [191]. In the context of this study, it is hard to understand how security protocols are violated without obtaining first-hand accounts from the banks CEOs, especially, since the focus of this study is on ISO/IEC27001 certified banks. In order to help overcome this initial challenge, the interview aspect of the primary data collection stage is set out based on the guidelines in [192]. Where it is suggested that open-ended questions allow detail responses that are necessary to understand a phenomenon of which little is known, as in the case of the compliant security model in this study. It is also suggested that a sequence of question and consistency should be maintained during the interview. All the suggestions are significant to the design of the interview questions for IS officers in this study (included in Appendix I). Responses from the interview questions are evaluated along with the IS survey design in literature, to help develop the survey questions in this study.

Survey: Survey research methodology is generally applied to elicit important constructs from the phenomenon of interest and the best ways to measure those constructs [193]. Survey research has been suggested [194] to be most appropriate for research design if it satisfies four important aspects of research, all of which have been considered appropriate for the current investigation. The conditions are as follows:

- The question about the research interest is on “What is happening?” or “Why and How is it happening?”. In the context of this study, the quest is to understand what factors undermine compliant security in banking organisations.
- The control of dependent and independent variables are not either possible or desirable. This study uses the perception of compliant behaviour as a primary observation unit.
- The subject of interest must be explored in their natural settings. In the context of this study, individuals security compliant behaviour is explored with respect to their organisation settings.
- The subject of interest must occur in the current time or in the recent past. Ongoing compliant security behaviour in banking organisations is the phenomenon of interest in this study.

This study's survey is designed to capture how ISO/IEC 27001 compliant banks that take part in this study implements policies and how employees respond to situations within the context of information security. The survey questions are structured to provide numerical data that can be explored statistically, and yield results that can be generalised to some larger population. The recruitment strategy for this part of the work is based on a presumably representative sample and randomly selected bank employees. A detailed recruitment strategy is discussed later in chapter 4.

3.3.1.2 Secondary Data

Scientific Publications: Some of the secondary data obtained for this work comes from scientific journals, conference proceedings and white papers. For instance, through relevant behavioural theories, extensive personality research and experimental results, it is possible to obtain parametric variables for our models and simulations.

Data Breach Reports: Reports of data breach incidents obtained from independent studies, governmental department and other non-governmental organisations (NGOs) provides vital information essential to the understanding of the current threat landscape across organisations. For instance, the Verizon enterprise solutions' data breach investigation report [195] and the Ponemon Institute/IBM Security cost of data breach study [196] help identify technical security breaches, nature of security incidents and what triggers security breach in most cases. This information also helped to developed parametric variables for our models and simulations.

3.3.2 Modelling and Simulation-Based Approach

As mentioned earlier, modelling and simulation-based approach are essential for exploring complex real-world problems in an abstractive environment. In this study, different modelling and simulation approaches are applied to address each of the research questions. The following subsections describe the models and simulations used for different elements of this work:

3.3.2.1 PLS-SEM Model

As part of the efforts to answer research question 1, this study applies Partial Least Square Structural Equation Modelling (PLS-SEM) to test the model construct and the validity of the research measurement model. PLS-SEM can test both measurement and structural models and also has less stringent distribution assumption [197]. Similarly, the reliability of the model construct is tested through the measurement of Cronbach's alpha to establish the consistency of survey responses across the scale.

3.3.2.2 System Dynamic Model

To address the research question 2, System Dynamics Modelling is used to link hypothesised structure with the observed behaviour of model entities over a period. Ventana Systems (Vensim PLE) is a fully functional system dynamics software package that can be used to address a variety of problems, and the causal loop tracing enables accurate and fast analysis of model dynamics. In the context of this work, Vensim is applied to establish causal tracing, dependencies and dynamic relationships between different domain risk indicators and the overall implication for cybersecurity incidents.

3.3.2.3 MATLAB (Matrix Laboratory) Simulation Model

As part of the efforts to address research question 2, modelling and simulation are also conducted in MATLAB. Developed by MathWorks, MATLAB is a versatile and powerful multi-paradigm computing environment that allows matrix manipulation for problem-solving. In the context of this work, MATLAB is applied to simulate a matrix table of values for an employee. The output from the simulation is used to establish the susceptibility of the employee to violate security protocols.

3.3.2.4 Monte Carlo Risk Modelling (ModelRisk)

In order to address the research question 3, Monte-Carlo simulation is conducted using the 'ModelRisk' software. Model risk is a quantitative risk analysis tool that is entrenched with probability distribution functions to describe uncertainties about input variables. Within the context of this work, 'ModelRisk' is used to generate 3-point estimation based on thousands of possible scenarios, to address the security resource allocation problems.

3.3.2.5 Model Validation and Verification

All models require some forms of justification that it is fit for purpose. However, random variables make it hard for modellers to determine and reason about the behaviour of a model under unknown conditions; and check that it is a good fit [187]. Replacing random variables with deterministic ones can help ascertain if the model is behaving correctly [198]. When the behaviour representation of a model is known to be correct, then random

variables can be introduced using continuous time distribution. In the context of this study, the soundness of model assumptions is compared with simulation output from different models, under known conditions.

3.4 Research Ethics

It is important that when conducting research studies, the legal requirements of data protection and the confidentiality rights of research subjects are respected at all times [186]. There are many professional bodies that provide guidelines on research survey ethical conducts [199], all suggesting that ethical consideration in research is critical. There should be respect for organisations' autonomy while also respecting organisations concern for the safety of human subjects in the research. In this respect, this study includes important ethical statements in the recruitment method. Firstly, the issue of consent was addressed prior to the commencement of the survey exercise, making it clear that participation was voluntary, to which prior approval was received. Secondly, the collected data are confidential and anonymised; and lastly, the privacy of participants and organisations are ensured. In addition, at the end of the survey/study, links to the online survey tool is deactivated, as can be seen in Appendix VI.

3.5 Conclusion

This chapter introduced the research design, presented the research questions again and itemised the steps taken to address each of the research questions in this study. The chapter also presents the research methodology, touching on the research approach, data collection methods, modelling and simulation tools and the relevance of each element of the research methods to the research questions. The chapter also touched on the important ethical considerations of this study. The next section presents the research contribution focus of this thesis; covering the exploratory study results, developed methods and models that address the compliance, malicious insider and security resource allocation problems.

SECTION 2: DEVELOPED METHODS AND MODELS

This section introduces the core part of this doctoral work by presenting the methods and models developed to answer all the research questions in this thesis. Each chapter represents a substantial piece of work and contributions that complement the efforts to address compliant security problems, malicious insider problems and cybersecurity resource allocation problems. The breakdown of the chapters are as follows:

- Chapter 4: Security by Compliance and The Implications for Banking Organisations.
- Chapter 5: Exploratory Study of Compliance-Based Information Security Management in Banking Organizations.
- Chapter 6: System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis.
- Chapter 7: Malicious Insider Threat Detection: A Conceptual Model.
- Chapter 8: Towards Understanding Incentives and Security Investment Decisions in Information Security.

4 SECURITY BY COMPLIANCE AND THE IMPLICATIONS FOR BANKING ORGANISATIONS

“Amateurs hack systems; professionals hack people.”

-Bruce Schneier

This chapter has been published in Fagade, T. and Tryfonas, T. (2016) ‘Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks’, in Tryfonas T. (eds), Human Aspects of Information Security, Privacy, and Trust. Lecture Notes in Computer Science. Toronto, Canada: Springer, Cham, pp. 128–139. doi: 10.1007/978-3-319-39381-0_12. The paper was rectified by Dr Theo Tryfonas.”

4.1 Introduction

The ubiquitous and interconnected nature of information systems, coupled with the ever-increasing cyber-capabilities of adversaries, means that information security (IS) is central to the protection, dependability and management of information assets for businesses and organisations. Banking and financial organisations operate in a dynamic and complex environment where risk management is an endless game between system defenders and adversaries, such that, threats to critical assets could compromise capital gains, human resource, time and competitive advantage for businesses [200]. Organisations take measures to protect information assets, ensure business continuity and reduce the risk of security breaches by implementing information security guidelines and protocols.

In response to the increase in cyber security incidents on critical infrastructures, industry regulators make it a mandatory requirement for operators to implement security policies in accordance with industry standards and regulations. For instance, under the Executive Order 13636, the US Federal Government introduced a technical framework and regulation aimed at protecting critical national infrastructure (CNI) cybersecurity and buildings [201]. Likewise, the EU put forward a proposal for a specific European Directive relating to the CNI operators, in both private and public enterprises for the management and regulation of cybersecurity issues [74]. In banks and financial organisations, information security risk is part of the overall management of operational risk. Any failure to implement appropriate security controls is considered a compliance issue, which can attract sanctions from industry regulators [200]. Compliant security is the acceptance of external entity defined controls, in the form of corporate governance, legislative and industry regulations. However, compliance-based security is determined by factors like the level of organisation security control requirements, the adoption, application and interpretation of different standards within the context of specific need [202].

This chapter introduces the first phase of the compliant security study and the discussion in this pilot study explores the behavioural dimension of compliance with information security standards. Based on the review of past literature, this study focuses on the factors that are integral to compliant security in Nigerian banking organisations. Based on the recommendations of an established model of information security governance framework [48], discussed in the literature review, and the application of the “Broken Window” theory [203] [204] from the field of criminology, to shape the narratives of compliant security; the study proposes how information security may be embedded into organisation security culture in that context.

The rest of this chapter is organised as follows; Section 4.2 covers the research method where the research case selection, data collection, sample demography and survey development are discussed. Results and analysis are presented in section 4.3. Section 4.4 covers a case scenario of how to embed security into organisation culture, while section 4.5 covers the conclusion, research implication and suggestions for future work.

4.2 Research Method

In respect to the overview of research methodology described in chapter 3, the following sections describe the design approach, method, and steps taken to address the compliance element of this study.

4.2.1 Case Selection

In line with the purposeful sampling technique to identify the critical case, in order to test theory within a real-life context [205], the case selection for this study is based on four major commercial banking organisations in Nigeria (using Bank A, B, C and D as a pseudonym). The four banks (ABCD) provides financial services to the three tiers of Nigeria government (local, state and federal agencies), also operating in all the 36 states of Nigeria, some African States and in European countries. Recently (in 2015), under the directives of the CBN, banks A, B, C and D achieved the ISO/IEC27001 certification and

compliance statuses, thereby driving their ISP program through the certification guideline.

Prior to the CBN directives, there was not a single unifying certification status or standard adopted for the Nigeria banking industry. The norm was that different banks develop, communicate and enforce their Information Security Policy (ISP) programs through various initiatives. The four selected banks for this study are all considered appropriate to investigate the first research question of this thesis. The management contact in CBN was very supportive of this study as it provides the opportunity to gain an insight into the effectiveness of the compliance program.

4.2.2 Data Collection

The data collection stages are shown in Table 4.1, involving the banks A, B, C, D and the CBN was carried out over two weeks between January and February 2016. At the first stage of the data collection, a semi-structured interview was conducted with the CISOs of the banks, and in cases where the CISO is not available, the interview was conducted with the next most senior security manager. The CISOs understanding of the research context was vital to this study, and the interview responses were instrumental to the design of the survey questionnaire. A sample of the interview question is included in Appendix II.

Stage	Method	Contact	Output
Stage 1	Interview	CISO Bank A CISO Bank B Snr Security Manager Bank C CISO Bank D	Interview Responses
Stage 2	Survey Pre-test	CISO Bank A CISO Bank B Snr Security Manager Bank C CISO Bank D	Recommendation for adjustments & Approval
Stage 3	Online Survey	Bank A, B, C and D Employees CBN Employees	Survey Responses
Stage 4	Post-Survey Validity checks	N/A	Survey Data

Table 4.1. Data Collection Stages

Responses from the interview questions are analysed, then in conjunction with established constructs from IS surveys [206], [207], a survey instrument was developed to fit the research model in this study. The preliminary version of the survey questionnaire was pretested with the security managers for feedback on comprehension, wording and fit-for-purpose. The final version was deployed in the form of an online survey through Google Forms, targeting (potentially) 800 participants over 2 weeks. There were 507 total respondents of which 7 invalid responses were recorded, and the rest of the valid 500 responses were considered for this study.

4.2.3 Sample Demography

4.2.3.1 Demography

All the participants in this study are employees of the banks discussed in the previous sub-section are drawn from different units/job positions in our target population. The participants are categorised under the Executive/Senior Level Managers, HR and Administration, IT Department, Operations and Others. Although not captured in the survey questionnaire (but based on the feedback from the pre-survey interview), all the survey respondents have been working in the banks between two and over ten years. Importantly, also, the study focus is on generic employee approach to security compliance. Therefore, sample characteristics are not distinguished by gender or job tenure.

4.2.3.2 Sampling

Sampling is described as the systematic inclusion of selected cases in a research project [208]. since it is operationally and economically impractical to collect data from every single person in a given population, a sample of the population needs to be selected for generalisation purposes [186]. in that context, the sample selection for this study is based on the interest of the banks to take part in the study. In addition, each of the participating banks A, B, C, D and the CBN have more than 1000 employees; and all the participating banks

have been certified ISO/IEC 27001 compliant. Importantly too, all the banks are using ISO certification to drive information security awareness.

4.2.3.3 Sample Frame

The recruitment strategy for this work is based on random selection from a representative group of bank employees. In terms of the sample frame, important steps have also been taken to prevent/reduce sample bias by including various representative units in this study, i.e. various bank branches from different states in Nigeria. For instance, the sample frame is drawn from bank branches from different districts in Abuja (the Federal Capital Territory of Nigeria) and branches from different local government areas Lagos state (the Commercial Centre of Nigeria). It is also ensured that respondents are drawn from different departments within the banks.

4.2.4 Survey Development

Survey methodology can be used to study employees' opinion, attitude and behavioural patterns within the context of information security [209]. This study surveyed four banks in Nigeria to gain the understanding of how security awareness and employee behaviour impacts on policy compliance. The survey is designed to capture how compliance-certified financial institutions implement policies and how employees respond to situations in the context of information security. It is important to point out again that results are obtained anonymously for the survey element of this work; due to data protection issues and the participating banks' reluctance to share vulnerability information,

An online survey was adapted from the survey methodology described in [206], [207], [209], which provided insights on how to design information security survey questions, to maximise response rate and minimise error. The literature also provided insight on how to make questionnaire short, easy to read, comprehend and using appropriate languages. Again, rather than using one of the standard information security survey questionnaires, this study combined interview responses with the

adopted survey methods in [206],[207], to develop survey instruments that are presumably more focused to the participating subjects, as a regional case study.

The survey questions are divided into three parts; security culture statements, knowledge and awareness statements and demography. Security culture statement assesses the behavioural pattern of employees that could undermine the effective implementation of policies. Knowledge and awareness statement assess the understanding of security policy requirements, while the demographic question captures survey representatives for segmentation analysis.

Demography					
1) What is your job level/department in the organisation?					
Executive/Senior Level Manager		I.T Department			
HR & Administration		Other			
Operations					
Security Culture Statements					
2) Information Security interferes with job productivity.	1	2	3	4	5
3) You can share your password with other people if you trust them.	1	2	3	4	5
4) It is safe to open an email attachment if it is not in the spam/junk box.	1	2	3	4	5
Knowledge & Awareness Statements					
9) Your organisation has information security policy, and you know where to locate a copy.	1	2	3	4	5
10) Your organisation has provided security awareness and training to all employees.	1	2	3	4	5
11) You know how to identify and report suspicious/actual security breaches.	1	2	3	4	5
12) Information is permanently lost when files on hard drives are erased or formatted.	1	2	3	4	5

Table 4.2. Extracts from the online information security survey

The survey questions follow a Likert scale response model (strongly agree, agree, uncertain, disagree and strongly disagree), except for question 1, which only measures the survey demography. Table 4.2 shows an extracted sample of questions from the online survey, and a complete survey questionnaire is included in Appendix III. A breakdown of the survey instrument and the literature from which they are adapted is also included in Appendix IV. Survey tool chosen for this work is Google Forms, an online survey application that allows real-time responses, data collation and analysis. The survey was

conducted over two weeks, and respondents were invited to take part in the survey through email communication, following the initial clearance from each of the participating bank's CISO. Additional recruitment information is included in Appendix V.

4.3 Results and Analysis

The Likert-type 5-point scale system used in this study is applied based on the survey data analysis in [210], whereby the numbers assigned to the measurement scale are treated as interval data, from which different responses can be calculated to obtain a measurable outcome. In that respect, our data is analysed by assigning a range value from 1 to 5 for each of the survey questions categorised under the security culture statements and the knowledge/awareness statements. Such that, if a statement is true from a security standpoint, five corresponds to 'strongly agree' and one corresponds to 'strongly disagree'. Respondents are then analysed by demography based on collective points. The maximum score per respondent is 55 points, which implies good security behaviour and compliance, while lower scores down to the minimum of 11 points lean towards poor security posture and non-compliance.

The demography of respondents is shown in Figure 4.1. 15.8% represents the executive/senior manager level, 12.3% from the IT department, 14% from HR and administration, 40.4% from Operations and 17.5% represents other categories. Job functions of other categories include marketing, accountancy, risk management, sales and predictive analysis.

Results from the security culture statement and knowledge/awareness statements are shown in Figure 4.2. More than 50% of respondents' view security measures as an inconvenient add-on but agrees that security is a necessary part of the secured work environment. Organisations need to take extra steps in ensuring that employees view security measures as necessary part of job requirements.

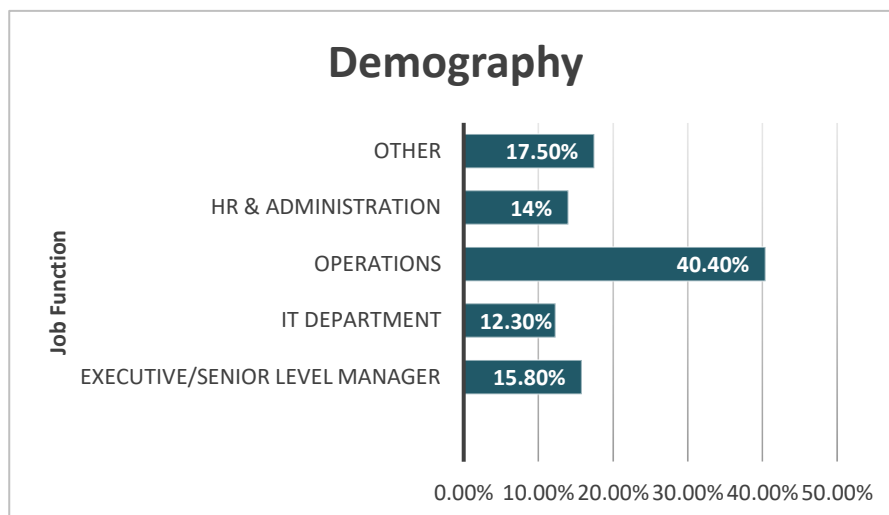


Figure 4.1. Demography of respondents

It is interesting to see that 12.1% strongly disagree and 9.1% disagree with the statement that their “organisations have information security policy, and they know where to locate a copy”. The implication of this result is that users who are not aware of organisation information security policy or know where to locate a copy can pose a significant risk. It could be that such users simply forget that security policy exists or find policy statements hard to understand.

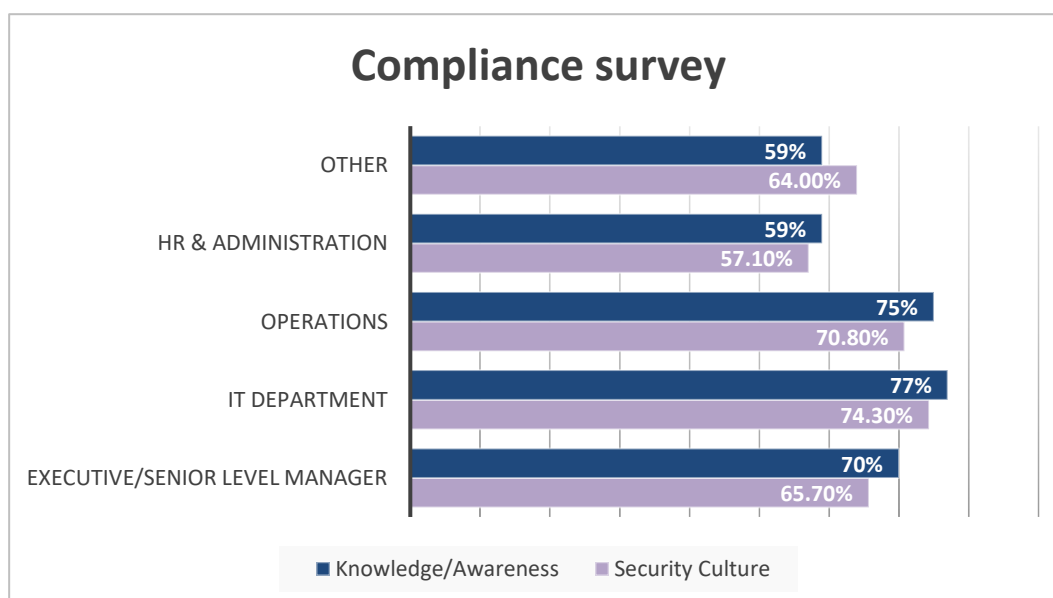


Figure 4.2. Information security compliance results

When asked if respondents know how to report actual (or suspicious) security incidents, 22.6% of respondents have no idea on how to do that. When users

cannot identify a potential security threat or whom to contact when there is a breach/compromise, such users may continue to expose information assets to threat by making further use of compromised devices. A significant number of respondents constituting 28% are misinformed on how to carry out secure disposal of sensitive electronic information. They assumed that data is lost permanently when deleted or when hard drives are formatted, this can pose a significant risk to an organisation. Forensic solutions that can erase end-of-life classified data need to be integrated into asset disposal policy.

The survey findings indicate that there is a high sense of security awareness, but secure practice and secure behaviour is low, which can have a significant impact on compliance. Although, not surprisingly, there seems to be higher evidence of compliance by employees in the IT department more than any other respondents. Considering that this survey is administered to employees from the financial institutions that have been certified ISO/IEC 27001 compliant, the study supports suggestions in literature [86], [87], [89], [90], that security by compliance is a far-fetched approach in terms of a holistic information security management.

4.4 Embedding Security in Organizational Culture

An organisation's compliance status is not necessarily a true indication that the desired changes in the behaviour of employees are achieved. However, given objective situations, it is unlikely that employees would be tempted to break the law if compliance is ingrained into organisation culture and everyday routine [211]. Embedding security into organisation culture is an important aspect of the compliance program. Security culture must adopt a top-bottom approach, starting with management buy-in and then gradually including everyone else in the organisation. It has been shown that top management buy-in and support has an enormous impact on policy enforcement and organisational culture [212]. The claim is also supported by behavioural theories like the "Broken Window" theory of policing [203], which suggests that inadvertently and seemingly unserious behaviour or incivility subsequently leads to serious crimes within the community. The translation of

this theory into practices in a cosmopolitan environment sees a dramatic decrease in high-level crimes when acts of misdemeanour were punished [204]. The application of this to security culture is that management top hierarchy is responsible for imposing measures which can have considerable influence on employee attitude, behaviour and motivation. By paying attention to little security details within an organisation, the big picture in the context of secured behaviour will begin to take shape. There has to be a demonstration of commitment by the management before there can be any success in integrating security in organisation culture.

4.4.1 Compliance Gap Mitigation: Data Security Scenario

In response to the gaps in the literature on the specific steps that could be taken to embed security into organisation culture [180], this section proposes conceptual principles and practical guidelines for the enforcement of employees' compliant behavioural changes. It suggests how compliant behaviour might be achieved by using data security case scenario and the information security governance framework [48]. Consider data security as an example; there are possible steps that can be taken to promote the concept of security compliance gaps mitigation. All traditional enterprises, organisations and government agencies, consider data as a critical and pervasive asset that requires top priority response. As such, most organisations understand the need for data security but may not necessarily know how to prioritize that for all employees. Since national or international data protection acts cover most organisations; this should be the starting point for embedding data security into organisation culture.

The first step to mitigating compliance gaps with respect to data security starts with the management top hierarchy, as illustrated by the security culture integration concept shown in Figure 4.3. Executive level sponsors and management top hierarchy should be able to understand, communicate and demonstrate the commitment to address the threats of information security in an organization.



Figure 4.3. Security culture integration concept

The second step is that management top hierarchy should also recognise the importance of security management organisations by accepting their organisations' legal/ regulatory obligations under the data protection laws of relevant jurisdictions (for instance, the ISO/IEC 27001 Standard, in the case the Nigerian banking organisations).

The third step is to express policy statements and specific guidelines for employee behavioural expectations. Data protection should then be included in organisation information security policy, which may further include point specific statements and policy subsets like regular data backups, and unauthorised use of portable devices on corporate computers. Policy subsets should show clear guidelines and best practices for ensuring data confidentiality, integrity and availability always.

The fourth step is that technical solutions that complement data protection policies can then be introduced as part of the security plan. Policy subset that safeguards data loss may suggest that employees regularly backup data, but compliance can be enforced if data backup becomes part of job functions. Technical solutions that can be leveraged as part of a data security strategy may just be a system, which forces or reminds the employee to do a data backup every day. Perhaps, if all employees that interact with information systems cannot log off after a day's work without completing backups to the central server, this function will become embedded in the organisation security culture where data backups become part of the job requirement, rather than being seen as an inconvenient security measure. Other policy subsets can then be applied to support compliance, for instance, disabling the USB ports on all organisation computers to control unauthorised copying of confidential information. Also, implementing a system that compels users to change passwords at intervals may ensure compliance and reduce threats posed by employees that are susceptible to social engineering. To avoid productivity challenges often brought about by extra layers of technical security; technical solutions can be introduced gradually while focusing initially on components that constitute everyday security issues. Therefore, employees that often see extra security steps as in-convenient add-ons may not be overwhelmed by the perception of reduced productivity, as a result of those extra security steps.

The fifth step is security program compliance monitoring; continuous auditing and compliance monitoring that involves technical and procedural controls, there is a better chance of timely response to identifying and managing compliance gaps. By identifying compliance gaps, security management programs can be set to promote and maintain security consciousness throughout the organization. Also, through improved resilience, security protocol violations could be significantly reduced. In the case of data security, improving resilience may include heightening employees' sense of responsibility surrounding data disclosure and unauthorised alterations.

The sixth and final step is user security management. Through user awareness and the reinforcement of ethical code of conduct programs, employees should become sensitised about company position on data protection. Organisations should communicate why data is vital to business continuity, how data loss may impact business and what measures can be taken to ensure data security. Most importantly, data security should become the responsibility of all employees and not only dedicated to a small unit of staff.

Through these measures, employees will become involved in the process of security whereby ***security requirements are incorporated into the organisation system architecture***. As employees learn to comply with the requirements of a policy, and observed behavioural change starts to emerge to the point where secure behaviour becomes second nature, a change in organisational culture which is also security driven will become evident. After that, management can begin to gently introduce other policy requirements in stages until the entire policy becomes embedded in the organisational culture. Through continuous assessment, the effectiveness of each security component embedded in the organisation culture can be measured over a given period. Security metrics may be based on how many times an organisation has recorded incidents of data loss since data backup. Employees will ultimately identify those changes as part of corporate culture and may not require extra motivation, reward or punishment to perform those functions. There are additional benefits of improved reputation and efficiency for organisations that have sound security practices integrated into its culture; ultimately such organisation will become compliant and secured.

4.5 Conclusion

It is arguable that security compliance is not a novel area of research. However, review of the literature confirms that compliance issues are still very valid and that the problem space still exists; even in recently ISO/IEC 27001 certified banking organisations. The findings of this study suggest that security by compliance as a campaign for information security assurance in the Nigerian financial institution is a far-fetched approach. In addition to standards, banking regulators should promote a holistic change of security culture across the sector. The general notion of compliant security is that organisations can defend security adequacy through compliant consistency. For instance, if an organisation is security focused rather than compliance and a security breach occur; it is not as easy to justify the organisation's security efforts, regardless of whether the organisation has a substantially grounded security program set up. This dynamic has led to a situation where many organisations opt for security through compliance, even though it may not be in the best interest of the organisation in the long run.

Certification is good, as it demonstrates compliance in highly regulated industries, but the downside is that business executives often focus on the cost of implementing compliance programs and once achieved; they operate under the assumption that compliance equates security. In practice, the control baseline may be enough for business executives and regulators, but it is insufficient in providing holistic security protection. For instance, one of the compliance requirements of the National Institute of Standards and Technology (NIST) is that data should be encrypted at the FIPS 140 level. If full disk encryption is carried out, but the encryption key is stored on the same disk, compliance requirements may have been addressed while still insecure. A secure and compliant approach would be full disk encryption and independent key management. Organisations may demonstrate compliance by focusing on the terms of frameworks and regulations but may still be not be secured in the context of general security initiatives as evident in the survey result of this study.

Policy development is meant to support employees and organisations with respect to the culture, workforce and the processes that must be adhered to fulfil business objectives. In reality, security policies are often developed with a myopic plan of actions by taking best practice and trying to overlay it into an organisation while the organisation may not have the tool, the capability or the maturity to implement those policies. Security professionals need to understand what type of behaviour and actions are currently taking place in an enterprise so that security policies that are more targeted and actionable can be planned. In particular, behaviours in a certain organisation like the banking and financial sectors should continuously be tracked and analysed to inform or help how policies should be developed or modified. It is believed that in addition to compliance, organisations need to cultivate information security culture because compliance is only a part of information security, and people rationalise compliant behaviour differently.

The strongest influence on organisation culture begins with the position of leadership. Leadership acceptance and active participation is a crucial aspect of information security. Executive level security representation and a change in management behaviour will reflect on employees' behaviour too. Information security channel of communication should be defined, and all employees need to be part of security. Also, some organisations have dedicated IT units that coordinate the implementation of information security policies, rather than promoting a sense of shared responsibility where security is a required function for everyone. If policy compliance comes natural to employees, it will be much easier for new employees to emulate acceptable behaviour through observation.

It is unlikely that information security culture can be covered by a single framework or few technical solutions. Future research may consider how to integrate other frameworks with the one adopted for this work and also suggest how human-centric technical solutions can be integrated into organisation security culture. In the next chapter, this work is extended by showing how compliance gaps may be reduced through the application of behavioural theories.

5 EXPLORATORY STUDY OF COMPLIANCE-BASED INFORMATION SECURITY MANAGEMENT IN BANKING ORGANISATIONS

*"If you know the enemy and know yourself, you need not fear the
result of a hundred battles."*

-Sun Tzu (The Art of War)

*This chapter has been published in the following journal and conference
proceeding:*

*Fagade, T. and Tryfonas, T. (2017a) 'Hacking a Bridge: An Exploratory Study
of Compliance-based Information Security Management in Banking
Organization', Journal on Systemics, Cybernetics and Informatics: JSCL,
15(Number 5), pp. 74–80.*

Fagade, T. and Tryfonas, T. (2017b) 'Hacking a Bridge: An Exploratory Study of Compliance-based Information Security Management in Banking Organization', in Nagib Callaos, Elina Gaile-Sarkane, Shigehiro Hashimoto, Natalja Lace, and Belkis Sanchez (eds) Proceedings of the 21st World Multi-Conference on Systemics, Cybernetics and Informatics (WMSCI 2017), vol. 2. Orlando, Florida: International Institute of Informatics and Systemics, Winter Garden, Florida. ISBN 978-1-941763-60-5., pp. 94–99. The papers were rectified by Dr Theo Tryfonas."

5.1 Introduction

The pilot study on compliant security in the previous chapter highlights that the problem space in organisations information security awareness (ISA) program is still very much valid. The preliminary study is consistent with other studies [111][211], that compliance-based security has the propensity for a heightened sense of false security and vulnerability perception. An absolute compliant security behaviour assurance from all employees is the holy grail for most organisations not only because security violations could sometimes be accidental but also because human behaviour is unpredictable, and the rational calculus of individual behaviour is dominated by benefits over risks [111]. In this respect, several kinds of literature have suggested the importance of applying behavioural theories to investigate employee compliance behaviour [213]. The argument is that behavioural theories will allow a deeper understanding of how employees rationalise security behaviour and shed light on the appropriate interventions that are most effective to improve compliance.

In this chapter, the behavioural dimension of information security policy compliance is explored by building on different models of human behaviour, including the deterrence theory and the rational choice theory. In particular, this work is approached through the lens of personality traits (a prominent postulation in the criminology domain), and the neutralization theory, to show that the level of systemic risk of security protocol violation in compliance-based security model can be explained by the level of linkages from the personality construct and the neutralization theory.

The research is conducted based on a case study of ISO/IEC27001 Standard certified banks, to empirically evaluate the link between cybersecurity protocols violation and how employees rationalise security behaviour. Based on the survey responses from banking organization employees and the application of Partial Least Squares Structural Equation Modelling (PLS-SME) analysis to test the causal model, the hypotheses and validate the survey samples, the study infers the importance of individual

security scenario effect as a vital element of compliance-based security. It is believed that this study will complement the broader body of information security research by highlighting the relevance of personality traits and neutralization techniques to compliance-based security management.

The rest of this chapter is organised as follows; Section 5.2 covers the theory development. Research model and hypotheses are described in section 5.3. In section 5.4, the research method, including the validation of measurement, a test of hypotheses and structural model analysis are presented. Section 5.5 focuses on the discussion of results. Finally, the conclusion is covered in section 5.6, where the study implications and the proposition for the next phase of work are presented.

5.2 Theory Development

Another gap identified as part of the literature review in chapter 2 is the role of personality traits and neutralization theory in organisation compliance programme when both factors are considered together in a single study. This study draws on prevailing human behaviour theories to explain how individual calculus may lead to the intention to violate organisation security protocols. Information security literature has shown that security culture and awareness is very significant to attitude formation that could either be favourable or unfavourable towards compliant behaviour [214]. Therefore, organisations conduct awareness training and comprehensive procedures for employees to forestall misconduct and security protocol violations [111]. However, because human behaviour is very difficult to lock down, and given the similarities between criminal behaviour in societal setting and information security violation behaviour in organisations, scholars have started to apply theories from criminology literature as the foundation for information security research [215],[115]. For instance, the Rational Choice Theory suggests that the decision to engage in criminal behaviour is subject to two different motivational elements; the benefits of the criminal act and the perceived cost of carrying out the act [216]. Hence, individuals have some

awareness of security protocol violation consequences, but makes a reasoned judgement based on the cost-benefit evaluation of the intended act [217].

Furthermore, individuals often exercise some restraints even in highly rewarding criminal situations, as informed by the Deterrence Theory. When faced with the conscious choice to violate protocol or commit crime, deterrence theory suggests that based on the fundamental rationality of human; only when the act is rewarding would that choice be made, but when the perceived certainty and severity of sanctions against the act are greater, there would be less motivation to commit the same crime [218]. In that respect, some organisations introduce the elements of punishment and reward to influence security compliance. Equally interesting also, is how humans try to dampen their internalised guilt and justify non-compliance security behaviour. Deterrence mechanism is not always effective at curbing security protocol violations [115], because individuals tend to conceptualise personal norms and justify actions that are otherwise not acceptable, through the application of neutralisation techniques.

Neutralisation theory suggests that individual act of defiance or rule breaking can be rationalised by absolving from all sense of responsibility as to why the defiance act took place; this can be achieved either in response to cognitive dissonance as a precondition to the act, or to be free from personal sense of guilt after the act [219]. However, Self-Control Theory suggests that the potential to commit a crime may domicile in everyone but in the end, not everyone commits crime because of the individual differences in the ability to exercise self-control. Self-control ability is established early in life, and similar to the Personality Traits, it remains fairly stable throughout an individual's lifetime [220] and [104]. It is, therefore, safe to assume that the rational choice to violate security protocol is a function of individual and situational factors [221]. Hence [104] concludes that individual personality traits and the cross-level interaction with security scenario effect determine the propensity to violate security protocols. In the context of information security, this study adopts the technique of neutralization, personality traits and security culture

to test the causal relationship between theories and organisation security compliance programs.

5.3 Research Model and Hypotheses

The research model is based on three constructs; the personality traits, the security culture and the neutralization technique. Description of the three constructs with respect to this study and the hypotheses derived are as follows:

5.3.1 The Role of Personality Traits and Security Scenario Effects

Evidence from the literature has shown that individual personality traits described by the 'Big Five' psychological constructs of Openness, Conscientiousness, Extroversion, Agreeableness and Neuroticism (OCEAN), can reveal a significant aspect of human behaviour [104]. In the context of information security, it is suggested that individuals with the same personality traits react differently to the same condition depending on the associated security scenario effect like self-efficacy, sanction severity, sanction certainty and response cost [116]. Therefore, differences in compliant behaviour intentions are based on the cross-level relationship between personality types and the way we respond to the security scenario effect. For instance, as illustrated in Table 5.1, two different employees with 'agreeable' personality and Narcissistic personality are likely to violate security protocols, if, under security scenario effects, they both show a low sense of sanction certainty.

Personality	Notation	Security Scenario Effect
Openness	O	Low sense of sanction severity
Conscientiousness	C	Low sense of response efficacy
Extroversion	E	Low sense of threat severity, threat vulnerability and response cost
Agreeableness	A	Low sense of sanction certainty
Narcissism	N	Low sense of sanction certainty

Table 5.1. Cross-level interaction between personality traits and security scenario effects (McBride, 2012)

Similarly, an employee with openness personality but a low sense of sanction severity or another with conscientiousness characteristic but a low sense of response efficacy is likely to violate security protocols. Therefore, this study hypothesizes the following based on three types of personality traits, which are supported by literature [104]:

H1a: Personality trait of 'Openness' and a low sense of sanction severity can negatively affect compliant security model.

An individual that has the 'Openness' personality trait; anchors on being consistent and cautious, as opposed to being inventive and curious. If the person's situational factor is low sanction severity, the perceived harshness of the punishment associated with security protocol violation will be undermined.

H1b: Personality trait of 'Conscientiousness' and a low sense of response efficacy can negatively affect compliant security model.

A person with 'Conscientiousness' personality trait, anchors on being easy-going and careless, as opposed to being efficient and organised. If the person's situational factor is a low sense of response efficacy, the perceived effectiveness of organisational security policy will be undermined.

H1c: Personality traits of 'Extraversion' and a low sense of threat vulnerability can negatively affect compliant security model.

An individual that has an 'Extraversion' personality trait; anchors on being solitary and reserved, as opposed to being outgoing and energetic. If the person's situational factor is a low sense of threat severity, threat vulnerability and response cost; the perceived risk, seriousness of risk or the perceived consequences of security protocol violation will be undermined.

5.3.2 The Role of Neutralization Techniques

Neutralization theory, introduced by [222], suggests that most adolescents are dissuaded from activities that violate societal norms because of associated guilts and shames. However, in order to obtain episodic relief from moral

constraint, individuals adopt the technique of neutralization to offset their guilt and freely engage in delinquency without impacting their self-image [223]. Researchers have applied neutralization techniques in various forms of rule-breaking or deviance behaviour that are not necessarily criminal [115]. Neutralization theory provides explanatory insight into how people are able to justify and break loose from restrictive societal norms and are able to rationalise rule-breaking actions without remorse [224]. Neutralization techniques have gained increasing appeal from behavioural scientists to understand and mitigate workplace deviance. The five neutralization techniques outlined in [222] are: 1) denial of injury, 2) denial of responsibility, 3) appeal to higher loyalties, 4) denial of victims, and 5) condemnation of condemners.

This study considers three neutralization techniques within the context of Information Security (IS) and hypothesizes the following, which are also supported by literature[222]:

***H2a:** Denial of Responsibility negatively affects compliant security model.*

Denial of Responsibility: this is a technique adopted to justify security risk behaviour by acknowledging that although certain actions are wrong, the offender claims that the situation is forced upon them and they had no choice. This could be a case of taking home sensitive corporate data in the bid to meet up with project deadlines.

***H2b:** Denial of Injury negatively affects compliant security model.*

Denial of Injury: this technique is a case whereby an offender admits to the violation of security protocol but try to justify his action by assuming that, no one is harmed because of his action. A typical example of this technique in IS context is the sharing of passwords with colleagues.

***H2c:** Blaming the Victim negatively affects compliant security model.*

Blaming the Victim: with this technique, an offender acknowledges that there may be some damaging consequences associated with risky behaviour, but the

offender blames the victim, e.g. an organisation, a manager or a supervisor as the reason for his action. An example of this in IS context is the installation of unauthorised software to access restricted websites on corporate networks.

5.3.3 The Role of Information Security Culture, Knowledge and Awareness

The general assumption is that training and awareness, as well as security culture, can counteract individual neutralization technique, leading to significant improvement in organisation compliance level [225]. In that respect, and also based on the pilot study in chapter 4, this study hypothesises that:

***H3a:** Security culture positively affects actual compliance level.*

A strong information security culture helps to subconsciously modify employees' intention from the evaluation stage to the execution stage, whenever the security policy violation is contemplated [9]. Security culture is therefore vital for managing organisational security compliance programs.

5.4 Research Method

The survey methodology for this study is based on the same approach discussed for the study in chapter 4; it covers the same banking organisations and the same number of respondents. In order to avoid unnecessary duplication, the reader should refer to sections 4.2.1 (case selection), 4.2.2 (data collection), 4.2.3 (sample demography) and 4.2.4 (survey development) in chapter 4 of this thesis. However, the survey instrument in this study is adapted from the literature on personality traits and the techniques of neutralization studies, in the context of information security.

5.4.1 Survey Development

The survey questions are divided into three constructs; personality traits, neutralisation techniques and security culture based on the hypotheses described earlier. There are also sixteen measurement items developed for the three constructs. Also, all the constructs are measured with multiple items on

the 5-point Likert-scale response model (strongly agree, agree, uncertain, disagree and strongly disagree) as described in chapter 4. It is important to note here that six of the measurement items relating to the constructs under personality traits are adopted from the studies of [104], [224]. Also, another six measurement items relating to the construct under neutralization techniques are adopted from [206], [76]. The last four measurements under the knowledge and awareness construct are included from the survey instrument in chapter 4. A copy of the survey measurement model and the literature from which they are adapted is also included in Appendix VI.

5.4.2 Validation of Measurement

Validation and reliability test of the result as shown in Table 5.2 follows the recommendation of data measurement goodness-of-fit in the literature [197], [226], while the measurement constructs and survey items are also tested for cotemporary recommended goodness-of-fit criteria based on PLS-SEM.

Latent Constructs	Indicators	Loadings	Composite Reliability	AVE
Low sense of sanction severity (LSS)	LSS1	0.76	0.77	0.63
	LSS2	0.82		
Low sense of response efficacy (LRE)	LRE1	0.89	0.85	0.74
	LRE2	0.82		
Low sense of threat vulnerability (LTV)	LTV1	0.90	0.88	0.78
	LTV2	0.87		
Denial of Responsibility (DR)	DR1	0.80	0.72	0.57
	DR2	0.69		
Denial of Injury (DI)	DI1	0.92	0.94	0.88
	DI2	0.95		
Blaming the Victim (BV)	BV1	0.91	0.93	0.86
	BV2	0.95		
Security Culture (SC)	SC1	0.95	0.94	0.88
	SC2	0.92		
	KA1	0.64	0.79	0.66
	KA2	0.95		

Table 5.2. Latent Variables validity and reliability measurement

To ascertain error-free, construct reliability, and internal consistency of result, values for the composite reliability (C.R) index for all constructs are assessed. Composite reliability is obtained by combining all the true score variances and covariances in the composite of indicator variables, and by dividing it by the total variance in the composite. C.R is used to check the internal consistency, which should be greater than the benchmark of 0.7 to be considered adequate. In this result, the C.Rs are higher than the critical threshold of 0.70, indicating adequate reliability for all constructs as can be seen in Table 5.2 and Figure 5.1 respectively. In order to accept the criteria of indicators reliability, the outer loadings are expected to be greater than 0.70. Although, in terms of the relevance of indicators examined through p-statistic. The p-value of the two indicators from two different constructs are not significant. However, when the outer loadings of these constructs are examined, they are both above the 0.70 that is recommended for all indicators; which are conditions suggesting that the indicators can be kept in the model [197].

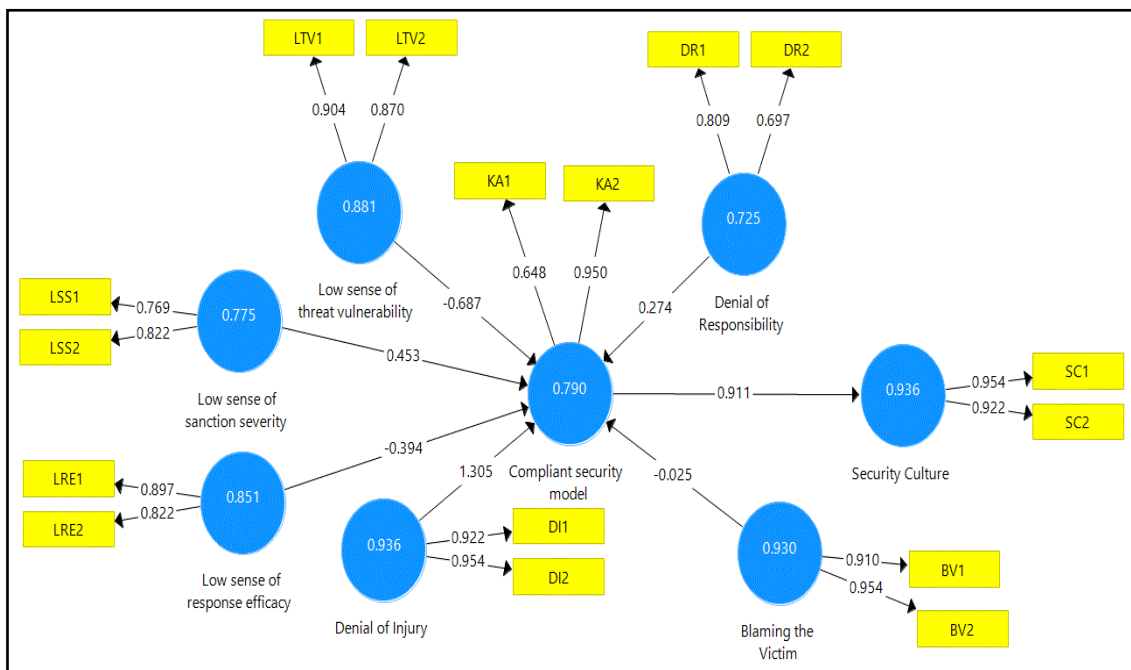


Figure 5.1. Structural Equation Model Results

Similarly, the measure of convergent validity based on the average variance extracted (AVE) for each construct exceeds the recommended 0.5 threshold criteria. The measurement items discriminant reliability assessment for almost all samples produced acceptable results. In addition, the loadings for all indicators are above 0.70, except for DR2 and KA1, which are very close to the recommended threshold at 0.69 and 0.64 respectively. Hence, we conclude that contemporary recommendations for the convergent and discriminant validity have been met.

5.4.3 Structural Model Analysis

All hypotheses are tested to measure the effect of neutralization and personality traits alongside different variables on the compliance-based security model. Further data analysis is conducted with IBM SPSS Statistics 23.0 [227] and SmartPLS 3.0 [228] packages. In addition, the t -statistics is calculated by conducting bootstrapping with 3,000 subsamples as a non-parametric re-sampling procedure, to evaluate the significance of the data coefficient. Table 5.3 shows the structural model result including the path coefficient for all hypotheses and the significance of the path (p-value).

Hypothesis	Path coefficients	t-value	p-value
H1a: LSS→ Compliant security model	0.45	2.42	n.s.
H1b: LRE→ Compliant security model	-0.39*	1.95	P<0.01
H1c: LTV→ Compliant security model	-0.68***	0.18	P<0.01
H2a: DR→ Compliant security model	0.27**	2.47	P<0.05
H2b: DI→ Compliant security model	1.30***	3.64	P<0.01
H2c: BV→ Compliant security model	-0.02	0.17	n.s.
H3a: SC→ Actual Compliant Level	0.91***	2.99	0.01

Note: n.s. not significant ***p<0.01 **p<0.05

Table 5.3. Findings on structural relationship showing path loadings and t-values

As hypothesized, this study found that H1b, H1c, H2a, H2b, and H3a are supported, while H1a, H2c are not. This implies that the compliance-based security model is significantly influenced by neutralization techniques, especially DR and DI in this case. Similarly, personality traits and cross-level interaction with security scenario effects have a direct bearing on the effectiveness of compliance-based security model. This result is also supported by the results obtained in [224], [229], although, this work is based on slightly different constructs.

5.5 Discussion of Results

The results of this study show the extent of coping with the appraisals of a security violation. In terms of personality traits and the interaction with security scenario effects, the result shows that both conscientiousness personality with a low sense of response efficacy **H1b** ($p < 0.01$); and extraversion personality with a low sense of threat vulnerability **H1c** ($p < 0.01$), have a weak negative effect on the compliance security model. This result is consistent with the study in [104], and also indicates that employees with a limited appraisal of the vulnerabilities that are introduced by non-compliance may have a higher chance of violating security protocol.

However, the openness personality with a low sense of sanction severity **H1a** is not supported in this study. This is contrary to the results of [104], and also indicates A possible explanation for this is that, while the personality of openness on its own does not necessarily mean that an individual is more or less likely to violate security protocol, individuals with different personalities also interact differently with the same situational factor [104], thereby suggesting that personality/security scenario should be evaluated on individual levels.

In terms of the neutralisation techniques, the results also indicate the importance of personal norm and individual rationale on the compliant security model. The results show that two of the neutralisation techniques; 'Denial of responsibility' **H2a** ($p < 0.05$) and Denial of injury' **H2b** ($p < 0.01$) have weak negative effects on the compliant security model. This is consistent with

other studies [10], suggesting that the neutralisation construct in this study indicates possible employee compliance violation intentions. Again, the 'blaming the victim' technique **H2c** is not supported in this study. The possible explanation for it is that while some employees may try to neutralise non-compliant behaviour, it is also possible that the employees could view themselves not to be at fault at all [230].

In terms of security culture, this study emphasises the important role of security culture in the management of organisation security compliance programs. The study shows a strong positive effect of significant impact on the compliant security model; thereby supporting **H3a** ($p < 0.01$). An organisation with a strong security culture is more likely to have a sustainable ISA program. This result is consistent with previous studies [231],[121] on the persuasion and improvement of employee security compliance that can be achieved due to strong organisation security culture.

The findings in this study support most of the hypotheses. Hence, the conclusion is that in response to research question 1, security by compliance is not adequate for organisation security management because of the variation in individual personality traits. Similarly, employees sometimes internalise elements of the neutralization techniques to justify non-compliant behaviour. Therefore, security managers should consider the links between personality types and personal norms as part of risk management, to determine if they strengthen or constrain the compliance security model.

5.6 Conclusion

Human factors continue to represent the gap between processes and technology, and there is no difference between malicious intent, negligence or external attacks regarding diminishing IT functions. There is no guarantee that employees will comply with policy requirements and there is insufficient understanding of the risks posed by users of information assets when behaviour variation is narrowed down to individuality.

Organisations can implement the most stringent security policies, but performance is mostly down to users. Cybercriminals would rather target authorised users who already sits within an organisation, than having a crack at multiple layers of external facing firewalls. That is why Organisations continue to device measures and other discipline mechanisms in order to deter non-compliant security behaviour. Unfortunately, the anticipated objectives in this respect are not always attained. Deterrent actions, through reward or punishment, has been shown to fail in organisations. Again, contrary to perfect rational assumption, punishing employees for accidental misuse or negligence may yield negative consequences. Besides, it is impractical, time-consuming and expensive to monitor employees continuously in order to enforce or deter certain behaviours. Without a grounded insight into the understanding of employees' motivation, deterrent measures as a means to address insider threat may not necessarily work.

Although this study is qualified by some limitations, the result highlights the importance of personality traits and neutralisation techniques in the design of organisational security policies. It is shown that, with respect to employee's personality dimension and security scenario effect, Low sense of sanction severity (LSS) and Low sense of response efficacy (LRE) negatively affects compliant security model. Similarly, in the context of neutralization technique, we show that Denial of Responsibility (DR) and Denial of Injury (DI) negatively affects compliant security model. However, for both personality trait and neutralization technique, the results have not been able to support the hypothesized negative relationship for a Low sense of sanction severity (LSS) and Blaming the Victim (BV) respectively. Nonetheless, it has been shown in this chapter that individual attributes and norms can influence the intention to comply with cybersecurity policies. Therefore, when organisations develop policies, the security awareness need of each employee should be factored into customized training programs. It is believed that this study will have a broader implication for security managers and researchers alike.

6 SYSTEM DYNAMICS APPROACH TO MALICIOUS INSIDER CYBER-THREAT MODELLING AND ANALYSIS

“Cyber-Security is much more than a matter of IT.”

-Stephane Nappo

*Part of this chapter has been published in Fagade, T., Spyridopoulos, T., Albishry, N. and Tryfonas, T. (2017) ‘**System Dynamics Approach to Malicious Insider Cyber-Threat Modelling and Analysis**’, in Tryfonas T. (ed.) *Human Aspects of Information Security, Privacy and Trust. HAS 2017, Lecture Notes in Computer Science*, Springer, Cham, pp. 309–321. doi: 10.1007/978-3-319-58460-7_21. The paper was rectified by Dr Theo Tryfonas.”*

6.1 Introduction

The high complexity of information systems along with the socio-technical nature of insider threats require a robust mechanism that can fuse numerous detector alerts, to establish and analyse patterns as a precursor to threats [3]. This is particularly important because when activities are performed to varying degrees by both benign and malicious insiders, the accuracy of isolated detector alert becomes uncertain. As explained in the previous chapters (4 and 5), the most significant challenge to organisations security efforts are the employees, and predicting human behaviour is a hard problem. It is shown that compliant security also falls short of providing a complete solution to this challenging problem because employees rationalise their behaviour differently. Even, Standards expect employees to behave within a certain frame of reference, which is not always the case, especially for determined malicious employees. Therefore, addressing malicious insider cyber-threat requires a more dynamic approach for analysing patterns as a precursor to threat, perhaps, a holistic, interdisciplinary approach that blends technological, psychological and organisational elements of the insider threat problem is required [232]. Following the literature review in chapter 2 and the gaps identified therein, this problem space is addressed in the current study through the application of system dynamics model.

6.1.1 Why System Dynamic Models?

Literature shows that security safety failure of any kind is mostly preceded by certain indicators [3]. For instance, the publicised software time bomb incident at Omega Engineering. A resentful employee of Omega intentionally destroyed the company's NetWare computer network, costing irreparable damage worth millions of dollars. The incident was said to have been preceded by many indications that the malicious insider intended to attack [233]. Hence, a system that can recognise and analyse the pattern of these indicators are necessary. The challenge, however, is that to have a system or a model of this nature, a modeller needs data. It is common knowledge how difficult it is to obtain real information about security breaches, including methodologies and

effect of attacks. This is why scholars continue to argue for the need to make cyber-attacks public, and that secrecy only aids the attackers [234]. However, system dynamic models can overcome cybersecurity data challenges because, rather than incident specific data about security breaches, the model aggregates data stocks and flow in quite an abstractive nature [3]. System Dynamics Modelling can be used to link the hypothesized structure with the observed behaviour of systems over a period of time, thereby allowing feedback to uncover certain types of endogenous phenomena [235]. The model is particularly useful for identifying causal structures leading up to attacks without necessarily having access to real cyber incident data [3]. This study, therefore, applies system dynamics modelling to understand the interrelationships between three distinct indicators of malicious insider activities, in order to determine the possibility of a security breach through developing trends and patterns. Risk indicators from different domains are aggregated as a precursor to a security breach, based on how the indicators influence one another.

The study combines the observable behaviour of actors based on the well-established theory of planned behaviour; technical footprints from incident log information and personality traits, based on the 'Big Five' personality model [104]; to demonstrates how system dynamics as a risk modelling approach can flag early signs of malicious insider threats, by aggregating the associative properties of different risk elements. The structure of this chapter is as follows; an overview of the model interconnected risk domains is presented in section 6.2. The methodology and simulation environment including model assumptions, analysis and results are presented in section 6.3, while section 6.4 covers the conclusion and discussion on future work extension.

6.2 Overview of model interconnected risk domains

For the purpose of this work, the model of malicious insider detection takes into account the personality, the behavioural and the technical risk indicators. Simulating multiple indicators of risk, based on the activities of an employee

illustrates a broader implication for a holistic information security management. Insider threat detection requires proactive analysis of multiple trigger factors far beyond network analysis alone. Hence, the idea of interconnected domains approach is based on the notion that different elements of risks are inextricably linked, therefore making each contributing factor a function of the malicious insider problem.

6.2.1 Personality Risk Indicators

Although personality traits are relatively stable through individuals' lifetimes, the ability to establish a statistically significant relationship between various personality profiles can provide guidelines for implementing security protocols that meet individual needs in a diverse workforce [104]. There are different ways of assessing personality types based on the five-psychological construct of Openness, Conscientiousness, Extroversion, Agreeableness and Narcissism (OCEAN). Some methods involve the use of measurement instruments like survey questionnaire and the NEO PI-R test [117]. However, people also reveal certain attributes through social media platforms, relating to psychosocial states like anxiety, debt, adjustment disorder and medical conditions, from which psychosocial risk factors could be drawn. For instance, by using the publicly available information on Twitter alone, it is possible to predict personality trait to within 11% [236], because certain words tend to be repeatedly used, leading to a pattern that can be correlated with a specific personality trait. Also, some studies [237] added that, through category-based textual analysis of browsing behaviour and webpage content, the Linguistic Inquiry and Word Count (LIWC) dictionary method could be applied to linguistically group and link some terms, from which personality traits can be profiled.

Other work claims that employees do not only transfer offline behaviour to online social network platforms, but there is also evidence to suggest a connection between the excessive use of social media and narcissist personality trait [238]–[240]. For instance, self-promoting contents combined with a high level of online activities are also strongly correlated with low self-

esteem, malevolent system use, narcissist personality and delinquent behaviour [241]. The personality trait of Openness is linked to being susceptible to phishing, while narcissism, agreeableness and excitement seeking is linked to insider threat and antisocial behaviour [121], [237]. Furthermore, the work described in [104] suggest that personality is a direct determinant of intention, individuals with different personality traits are more likely to react differently to the same security scenario, threats and organisation sanctions based on their perception of deterrence, protection motivation or efficacy factors. Therefore, when the 'Big 5' personality traits are treated as the moderating factor to security scenario effect (efficacy factors), they can reveal how likely it is for an individual to violate security protocol, as shown in Table 6.1.

Individuals who are <u>less</u> likely to violate cybersecurity protocol	Individuals who are <u>more</u> likely to violate cybersecurity protocol
<ul style="list-style-type: none"> • Open individuals with a low sense of Self-Efficacy • Open individuals with a low sense of Threat Severity • Open individuals with a low sense of Response Cost • Conscientious individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Sanction Severity • Agreeable individuals with a low sense of Self-Efficacy • Agreeable individuals with a low sense of Sanction Severity • Neurotic individuals with a low sense of Self-Efficacy 	<ul style="list-style-type: none"> • Open individuals in general • Open individuals with a low sense of Sanction Severity • Conscientious individuals with a low sense of Response Efficacy • Extroverted individuals with a low sense of Threat Severity • Extroverted individuals with a low sense of Threat Vulnerability • Extroverted individuals with a low sense of Response Cost • Agreeable individuals with a low sense of Sanction Certainty • Neurotic individuals with a low sense of Sanction Certainty

Table 6.1. The Big Five personality traits and security scenario effects (McBride, 2012)

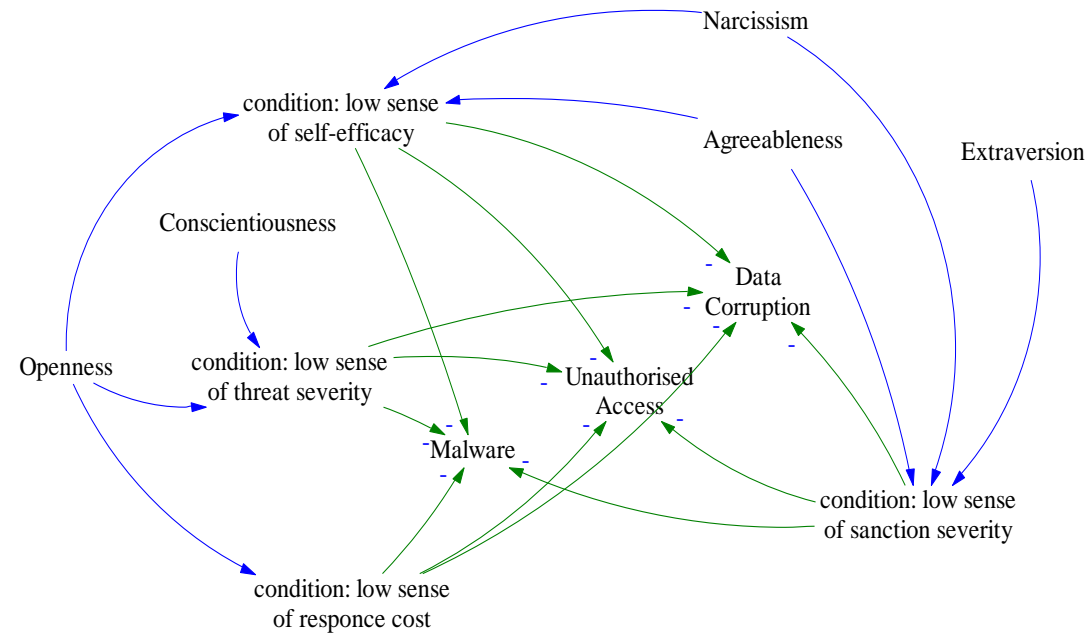


Figure 6.1. Cybersecurity risk reduces due to personality traits under specified conditions

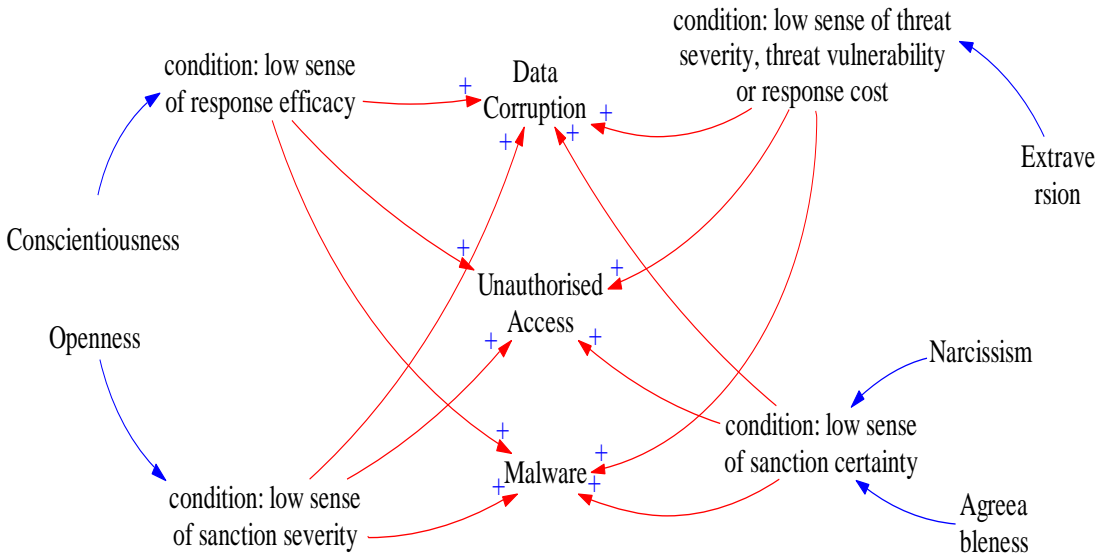


Figure 6.2. Cybersecurity risk increases due to personality traits under specified conditions

In order to dynamically model the effect of personality on efficacy factor conditions and security protocol violation, consider the generic personality model shown in Figure 6.1 and Figure 6.2, developed from the personality types described in [104]. It can be seen from Figure 6.1 that an individual with 'Extraversion' personality trait, but with a low sense of sanction severity, is less likely to violate cybersecurity protocols than an individual with 'Openness' personality trait and low sense of sanction severity shown in Figure 6.2. Likewise, as shown in Figure 6.1, an individual with 'Extraversion' personality but with a low sense of threat severity, threat vulnerability or response cost is more likely to violate security protocols than an individual with 'Conscientiousness' personality trait with a low sense of threat severity or someone with 'Openness' personality trait with a low sense of response cost, shown in Figure 6.2.

6.2.2 Behavioural Risk Indicators

Theory of planned behaviour has its foundation on a number of constructs, and it helps us to understand the reason for the deliberate behaviour. It explains why it is hard to change how a malevolent insider perceives security protocols. Security managers may provide training, implement policies and guidelines but users may not necessarily comply, even when it is mandated. An important aspect of the theory of planned behaviour is that, given a degree of control over events, people are expected to carry out their behaviour. However, intentions can change on the emergence of new information [242]. Previous behaviour and actions of the malevolent user can help inform future actions, but the challenge is that behaviour could change if triggered by external events. Also, behaviour may not be readily quantifiable if there are irregular intervals between malicious activities or there are no prior established patterns.

Behavioural theories provide guidelines on how behaviour may manifest in different stages of an insider threat scenario through certain indicators. The theory of planned behaviour suggests that a person's intention, perceived behaviour towards crime, subjective norms and attitude are key factors in predicting behaviour [106]. Pre-employment background checks,

360 profiler and other profiling mechanisms, may help to identify agents that constitute a behavioural risk, some of which may be unrelated to employment, like anxiety, breakup, depression, debt and medical conditions [243]. Psychological state is often evident in the way people behave, and behavioural risks can reflect through a variety of psychosocial risk indicators as shown in Table 6.2, describe in [135]. HR personnel are positioned to capture these behaviours and understand the severity, in terms of how the behaviours can undermine organization security efforts.

Indicator	Description
Disgruntlement	Employee observed to be dissatisfied with the current position, chronic indications of discontent.
Accepting Feedback	The employee is observed to have a difficult time accepting criticism or becomes defensive when the message is delivered.
Anger Management Issues	The employee often allows anger to get pent up inside; the employee has trouble managing lingering emotional feelings of anger.
Disengagement	The employee keeps to self, is detached, withdrawn and tends not to interact with individuals or groups.
Disregard for Authority	The employee disregards rules, authority or policies
Performance	The employee has received a corrective action that is based on poor performance.
Stress	The employee appears to be under physical, mental, or emotional strain or tension that the employee has difficulty handling.
Confrontational Behaviour	Employee exhibits argumentative or aggressive behaviour.
Personal Issues	The employee has difficulty keeping personal issues separate and interfering with work.
Self-Centeredness	The employee disregards need or wishes of others, concerned primarily with own interests and welfare.
Lack of Dependability	The employee is unworthy of trust; unable to keep commitments or promises.
Absenteeism	The employee has exhibited chronic unexplained absenteeism.

Table 6.2. Psychosocial risk indicators (Greitzer, 2010)

Although, some risks may not directly link psychological behaviour to a criminal background but may help address the psychological factors required to form group homogeneity [131], [135]. Based on 23 cases of insider threat in the banking and finance sector, 33% is due to personal problems that are unrelated to employment, like breakup and anxiety; 23% is due to revenge,

27% is due to debt, and 81% is due to financial gains [118]. In another report [96], based on a case study of 52 illicit cyber activities in the IT and Telecommunication sector; 33% is due intolerant to criticism, 57% involves disgruntled employees, 47% is revealed through overt behaviour, and 58% involves direct communication of threat online. Behaviour and external environmental influences can indicate early signs of cyber-security risks, as shown on the generic system dynamic diagram in Figure 6.3. The more individual exhibits one or more combinations of the behavioural risk elements, the more likely it is to violate cybersecurity protocols. Human resource staff are particularly well trained to apply observation techniques, recognize and report high scoring risk indicators as a predictor of anomalous behaviour.

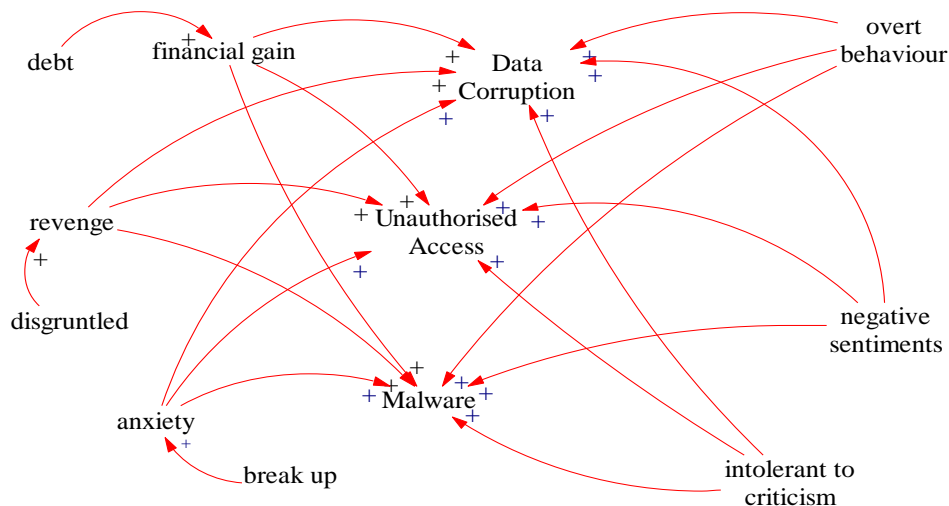


Figure 6.3. Cybersecurity risk increases due to individual's behaviour or external influence with negative psychological effects

6.2.3 Technical Risk Indicators

There are six categories of critical log information that can be used to identify suspicious activities. These include authentication, system and data change, network activity, resource access, malware activity, failure and critical error logs. Security tools like SIEM/log analysis, data access monitoring, intrusion detection/prevention systems (IDS/IPS) can be leveraged to provide administrators with sufficient information on suspicious activities [244].

Changes to configuration file binaries, network assets authentication and authorization log reports can be tracked to monitor employee activities. For instance, different patterns of system usage based on defined attributes can be combined with log information, job roles and privileges to create a profile for a regular user in a particular role. If there is an irregular pattern in the log information for a particular user compared to the activity of a regular user for the same role, then, that may suggest potential insider activities. A case study of 52 cyber incidents [96] shows that 57% of incidents are detected through system irregularities; of which 73% involves remote access logs and 57% involves unauthorised file access logs. Based on another study [95] involving 36 illicit cyber activity in the government sector, 24% of incidents are due to unauthorised privilege users, and 11% involves the installation of backdoors. Figure 6.1, Figure 6.2 and Figure 6.3 shows how technical risk may be influenced by the interplay of other variables like personality traits and behaviour.

6.3 Methodology and Simulation Environment

6.3.1 Model Analysis

System Dynamics can be used to link the hypothesized structure with the observed behaviour of systems over a period of time, thereby allowing feedback to uncover certain types of endogenous phenomena [235]. Ventana Systems Personal Learning Edition (Vensim PLE), a fully functional system dynamics software package, is used to conduct the simulation in this chapter. It is proposed that when behavioural, technical or personality risk, are considered in isolation, it may not be a true indication of the possible presence of a malicious insider. Irregular intervals between illicit cyber activities or inconsistent overt behaviour are difficult to apply independently as evidence of malicious insider. In order to prevent false positive triggers, each element of the risk indicators can be inextricably linked and modelled to draw more valid inferences. When risk factors are combined and observed as they change

over a period of time, developing patterns can provide significant confidence in identifying potential malicious insider.

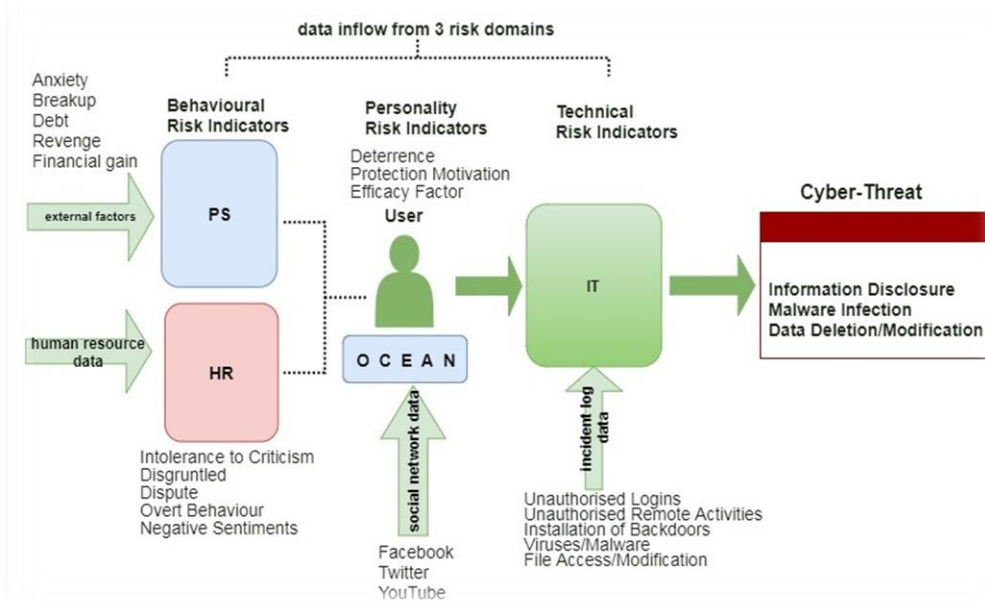


Figure 6.4. High-level abstraction of the insider threat modelling process

Consider the high-level abstractions for the conceptual model shown in Figure 6.4. Organisations can define an employee's 'normal' security profile based on different risk indicators, deterrence, protection motivation, efficacy factors and job roles. Employee activities are then monitored over a period of time e.g. monthly, based on combined data flow from three domain streams. Social network data can be leveraged to determine personality trait for a particular employee. This could be a contentious issue; however, we suggest that data from open social networks such as Twitter may be used legitimately and are made available by employees themselves. Human resource (HR) data provides input from constantly monitoring and analysing behavioural risk indicators for that employee, in addition to the employee's psychological state (PS). Monitoring psychosocial behaviour is crucial because it could be exacerbated by external factors that are not necessarily related to an employee's job. Likewise, incident log data obtained from the IT department is used to determine technical risk indicators.

In order to determine the security status of an employee, inputs from the external environment that forms PS are combined with behavioural risk factors from HR. The output from this can be influenced by the personality of a user. Then, depending on the personality of an employee and the employee's perception of deterrence, protection motivation and efficacy factors, the likelihood of a cyber-security protocol violation can be determined. For instance, people with 'Narcissistic' personality and low sense of sanction certainty are more likely to cause cyber leakage, espionage or delete critical system files, if associated PS and HR variables are true. Similarly, someone with 'Agreeable' personality with a low sense of sanction certainty is more likely to be susceptible to phishing, if associated PS and HR factors are triggered.

6.3.2 Model Results and Discussion

The dynamic relationship diagram in Figure 6.5 presents the stocks and flows that describes the dynamics between a person's behaviour, personality and the probability of a cyber-security incident (data corruption or unauthorised access), based on the generic system dynamics diagrams provided in Figure 6.1, Figure 6.2 and Figure 6.3. In particular, we consider behaviour as the combination of a person's psychosocial state (PS), sculptured by external triggers (e.g. breakup or debt), with employee's internal behaviour (e.g. intolerance to criticism or negative sentiments) as observed by the HR department. Negative internal behaviour combined with an unhealthy psychosocial state can increase the probability of a cyber-security incident. On the other hand, personality can play a twofold role; as shown in our generic model (Figure 6.1, and Figure 6.2) that depending on specific conditions (e.g. low sense of sanction severity or low sense of response cost), certain personality traits (e.g. Openness) can either increase or decrease the probability of a cyber-security incident (e.g. Malware).

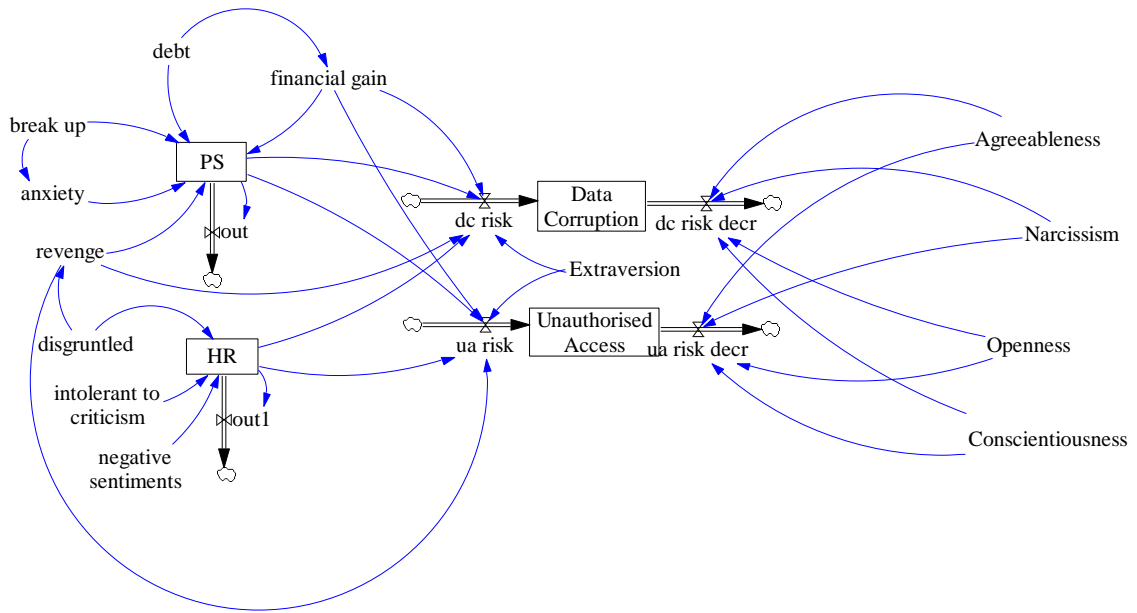


Figure 6.5. Dynamic relationship between personality, behaviour and cyber-security incident

In order to simplify the stocks and flows diagram for our model, an assumption is made that for the employee under consideration, apply the following conditions: “low sense of self-efficacy” and “low sense of threat severity”. Under these assumptions and according to our generic diagrams, ‘Extraversion’ increases the probability of a cyber-security incident while ‘Openness’, ‘Conscientiousness’, ‘Narcissism’ and ‘Agreeableness’ decreases it. These relationships are captured in Figure 6.5, where all personality traits except ‘Extraversion’ contribute to the decrease of the cyber-security incident risk. All variables in Figure 6.5 take values from 0 to 1. Figure 6.6 shows the probability of data corruption in time for different combinations. Before the experiment commenced, all personality traits are set to 1, and all internal behaviour and external psychosocial variables are set to 0. Then the following variables are changed: debt, intolerance to criticism, negative sentiments and O.C.A.N. (Openness, Conscientiousness, Agreeableness and Narcissism) and the model is run for various combinations, as shown.



Figure 6.6. Probability of data corruption in time based on personality

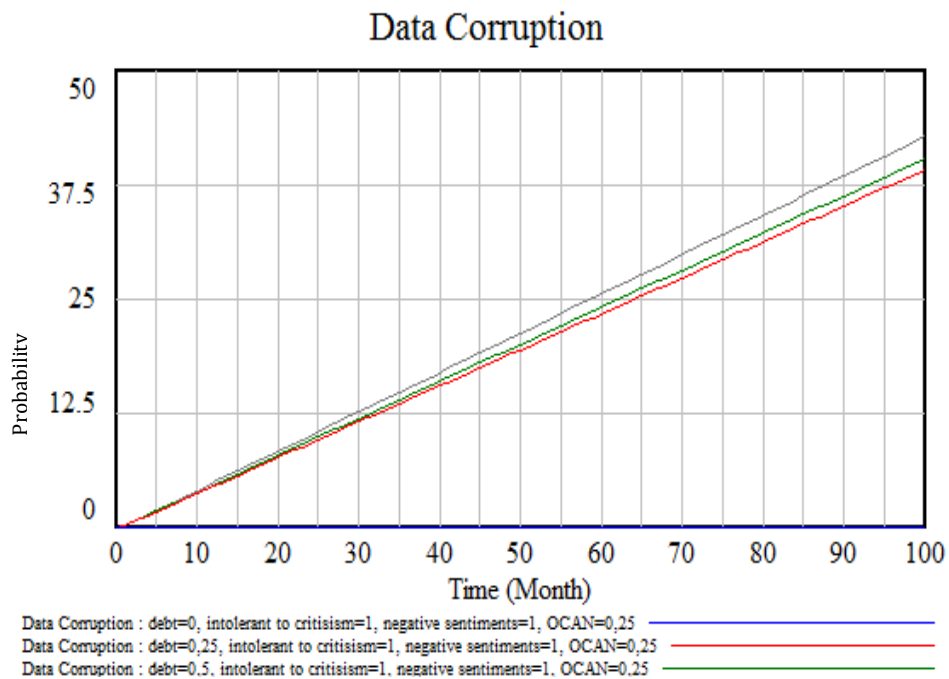


Figure 6.7. Probability of data corruption in time based on behaviour

As evident in [104], personality plays a vital role to cyber-security; the more open, conscientious, agreeable and not narcissist someone is, and depending on the associated deterrence, protection motivation and efficacy factors, the less likely it is to be involved in a cyber-security incident. However, as shown in Figure 6.7, keeping constant the personality traits may still result in different cyber-security risk levels caused by the effect of external inputs (in this case debt) on the employee's psychosocial state. All experiments were made taking into account a particular set of conditions described in [104]. By changing these conditions and according to the description of our generic diagrams in Figure 6.1, Figure 6.2 and Figure 6.3; changes in the personality would have different outcomes than the ones presented in Figure 6.5 and Figure 6.6.

6.4 Conclusion

This chapter describes a continuous feedback process for the detection of malicious insider cyber-threats, based on a system dynamics approach. Some of the critical challenges to combating insider threats are uncertainty, irregular behaviour, intervals between malicious activities and the exclusion of personality traits in the design of cyber-security protocols. Similarly, there is a distinct limitation to the application of technical measures alone in order to mitigate malicious insider threats.

This study seeks to gain an understanding of how the interplay between individual personality traits, inherent behaviour and external influences are directly linked to the violation of cyber-security protocols. It concludes that although personality traits differ between insiders, the motivation to violate or protect security protocols also varies for insiders with the same personality traits. Having the personality trait of one of the OCEAN elements does not make an individual more or less likely to violate security protocols, but the psychological states and the external episodic incident that triggers behavioural change can also contribute to the likelihood of acting maliciously. The argument is that personality and efficacy factor affect security violation, the effect of behaviour on security violation is also of equal importance. If there is an absence of detection capability for behavioural

changes or ‘anomaly’ digital footprints; it may actually suppress the threat detection capability that is based on personality traits alone. This observation is in line with the studies in [245], which argues that personality-based approach to profiling individuals may be limited by the way people actually manifest different levels of personality, at different times and to a different degree depending on what they set to achieve. It is believed that a model which is not inhibited by a strictly unilateral approach can significantly improve cyber threat detection.

This chapter shows that through combined behavioural analysis (HR) and externally triggered psychological factors (PS), technical footprints (IT) and personality types (OCEAN), the design and implementation of appropriate cyber-security protocols, should be based on a full understanding of insider psychological and security profiles. Similarly, providing generic cyber-security training and awareness programs without a deep understanding of employees’ psychological statuses is merely a one-size-fits-all approach that rarely ensures compliance. Based on this insight and as part of the future research, this study serves as the basis for the design of a conceptual model for insider threat, discussed in chapter 7.

7 MALICIOUS INSIDER THREAT DETECTION: A CONCEPTUAL MODEL

*“An accurate vision of digital and behavioural gaps is crucial for a
consistent cyber-resilience.”*

-Stephane Nappo

*“Part of this chapter has been published in Fagade, T. and Tryfonas, T. (2017c) ‘**Malicious Insider Threat Detection: A Conceptual Model**’, in Jaroslav Dockal, Milan Jirsa, and Josef Kaderka (eds) *Security and Protection of Information 2017*. Brno: University of Defence, IDET, pp. 31–44. The paper was rectified by Dr Theo Tryfonas.”*

7.1 Introduction

This chapter builds on the study in chapter 6 where the dynamic flow of insider risk indicators from different risk domains was discussed. In light of this, the current study proposes a conceptual model of insider threat prediction. Therefore, the narrative of the prior and the literature review are still consistent with chapter 6 and unnecessary repetition will be avoided in this chapter.

This chapter offers a different perspective to address the insider problem by drawing concepts from behavioural theory, personality profiling and digital trails to develop a conceptual model of malicious insider threat detection. In line with relevant research output on why trusted employees with elevated access continue to pose security challenges to organisation risk mitigation efforts, it is suggested that malicious insiders show certain personality traits [104], leave behind digital footprints and observable cyber risk behaviour [135] in advance of an attack. Instead of isolated treatments, our approach considers the intersection of different risk domains and aggregates risk scores from each domain as a predictor of malicious insider activities. The conceptual model of a malicious insider detection system discussed here combines threat indicators from different inter-related domains in order to prevent cyber risk while lowering false-positive thresholds and background noises. The model is based on hypothesised risk indicators supported with evidence from academic literature and subject experts' opinion. Concepts are drawn from the theory of planned behaviour, the 'Big Five' personality dimensions and technical anomaly detection, such that, different elements of threat that are inextricably linked from different domains are treated as a function of the malicious insider problem. The rest of this chapter is as follows; the background description of our conceptual model is presented in section 7.2. Method and preliminary design are covered in section 7.3, while section 7.4 covers the conclusion and future work.

7.2 Background Description of the Conceptual Model

An important consideration here is that due to the introductory and analytic modelling of this work, an in-depth analysis of the quantifying metrics and weighting factors assigned to each insider threat indicators are not covered. It should be noted that assigned weights are subjective and depend on the expertise of the human resources, data analytics, cybersecurity teams and the risk tolerance of each organisation.

Personality	Notation	Security Scenario Effect	Weight
Openness	O	Low sense of sanction severity	0.35
Conscientiousness	C	Low sense of response efficacy	0.21
Extraversion	E	Low sense of threat severity, threat vulnerability and response cost	0.45
Agreeableness	A	Low sense of sanction certainty	0.25
Narcissism	N	Low sense of sanction certainty	0.65
Technical	Notation	Alert Status/Count	Weight
Unauthorised logins	UL	1	0.28
VPN/Remote logins	VRL	2	0.36
Unauthorised Software Installation	USI	1	0.38
File Deletion/Modification	FDM	1	0.32
Viruses/Malware	VM	3	0.25
Behaviour	Notation	Alert Status/Count	Weight
Destructive Behaviour	DB	2	0.38
Intolerance to Criticism	IC	3	0.43
Security Violation	SV	2	0.32
Drug and Alcohol Abuse	DAA	3	0.45
Isolation and Seclusion	IS	4	0.28

Table 7.1. Risk indicators

In Table 7.1, weightings associated with the risk factors from different domains are provided, tables of risk indicators as shown are maintained by the administrator from each risk domain. In the case of technical and behavioural risk indicators, weighting values are assigned based on the alert status/count

associated with each risk element; while scenario effect parameters are the determinants of weighting values in the case of personality risk factor. For instance, in the technical risk domain, unlicensed/unauthorised software installation requires just a single count (one occurrence) and a weighting factor of 0.38, before that activity is recorded as a technical risk for a specific user. The rest of this section provides a brief description of each domain and risk factors considered for this work.

7.2.1 Personality Risk Factors

There are different methods and assessment tools like the Myers-Briggs Type Indicator (MBTI), Revised NEO Personality Inventory (NEO-PI-R), survey questions and social media profiling that can be utilised to measure personality traits based on the 'Big Five' psychological construct of Openness, Conscientiousness, Extroversion, Agreeableness and Neuroticism (OCEAN). Although, personality trait is fairly stable throughout an individual's lifetime, and it could be a key determinant of intentions [104], but studies also suggest that individuals with the same personality react differently to the same condition depending on associated security scenarios like self-efficacy, sanction severity, sanction certainty and response cost [116]. The personality risk factors aspect of this work is mainly based on the empirical studies conducted in [104], [116] and summarised in Table 7.1 by showing the cross-level relationship that exists between personality types and security scenario effects. Weight is assigned to the personality and security scenario interaction based on how likely or not it is, for an individual to violate cybersecurity protocol, as described in table 2.4 (Chapter 2) and table 6.2 (Chapter 6).

7.2.2 Technical Risk Factors

There are varieties of security tools [246]–[248] that can be deployed for network and host level assessment. Although most of these tools are based on the audit process that performs security checks against known vulnerabilities, they can also provide a snapshot of technical risk factors within an organisation. For instance, tools like the Security Information and Event

Management (SIEM)/log analysis and Intrusion Detection Systems (IDS) can provide sufficient information on the changes to configuration file binaries, access authentication logs and other anomalies from which a logical connection can be drawn about a user's activities [244]. This can allow system administrators to profile a normal user based on job roles and privileges, such that, if there is an irregular pattern in the log information for a particular user, compared to a typical user for the same role, then that may be an indication of potential malevolent insider activities. Table 7.1 shows some of the hypothesised cyber risks included in this model, indicating the alert status (count) for each situational risk factor and the corresponding weighting factor.

7.2.3 Behavioural Risk Factors

Although some behavioural risks like disgruntles, destructive behaviour and policy violations could be triggered by external factors which are unrelated to employment or criminal backgrounds like anxiety, breakup, depression and debt; but they may help address psychological factors required to form group homogeneity [131], [135]. Behaviour and external environmental influences can indicate early signs of cybersecurity risks, and the more individual exhibits one or more combinations of the behavioural risk elements, the more likely it is to violate cybersecurity protocols. Human resource staff are particularly well trained to apply observation techniques, recognise and report high scoring risk indicators as a predictor of anomalous behaviour. As with other risk factors, Table 7.1 shows the behavioural risk indicators, alerts status and associated weight factor considered for this study.

7.3 Method and Preliminary Design

The model considers different types of situational risk factors in an organisation, i.e. behavioural, personality and technical/system-level risk elements from three different domains; the human resource (H.R), personality profiling (P.P) and technical (I.T) domain respectively. In line with evidence from literature, this study is based on the premise that when technical risk factors are considered in isolation, the result is susceptible to false positives and cannot be a strong indication of malicious insider activities. However, when an agent is suspected of violating organisation security protocols, other situational risk factors can be aggregated to detect with increased accuracy, the pattern of activities that can characterise a malevolent insider. By using this approach, organisations can build employee profile and define a 'normal' risk threshold (R.T), based on threat indicators and the job role for that employee. To determine R.T, consider the high-level abstractions for the conceptual model shown in Figure 7.1. Data flow from the 3 domain streams are combined and processed for a single value output. Data from social network platforms, surveys, 360-degree profiler and other personality tests can be leveraged to obtain personality trait for an employee. Also, by continually monitoring and analysing behavioural risks and psychological state for that employee, the human resource (H.R) can provide data for a given time, indicating the behavioural risks for that employee. Similarly, incident log data obtained from the IT department can provide input for the employee technical risk indicators. These inputs can then be analysed to determine an acceptable R.T for that employee.

Employee activities are then monitored over a period, e.g. monthly, and risk score (R.S) is compared to a defined risk threshold (R.T). If there is a significant deviation from the 'normal' pattern in each time period, the system flag warning triggers which signify a risk status for that employee, then the employee could be placed under close supervision. Thereafter, the organisation can invoke a standard threat mitigating procedure. If the risk threshold is not matched or exceeded, risk status will not be triggered, and observation simply continues.

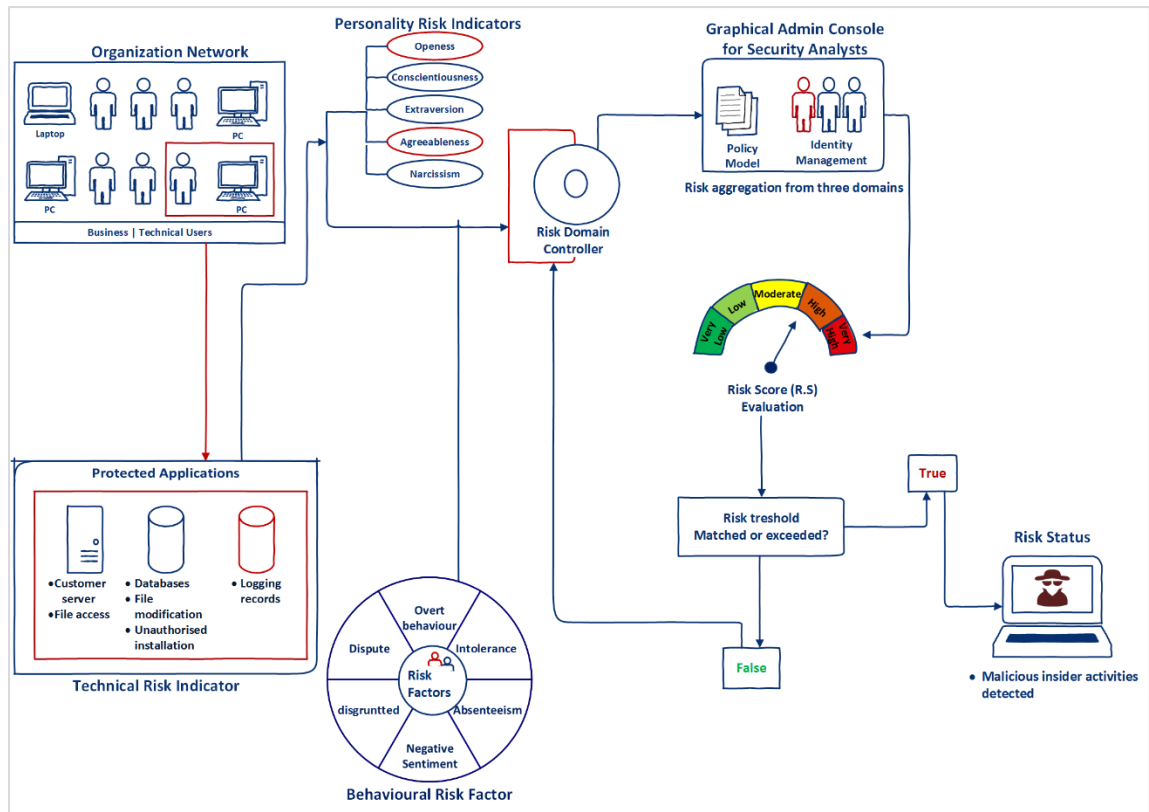


Figure 7.1. High-level abstraction of the insider threat modelling

The key assumption in this model is how weighting values are assigned to risk elements of the threat indicators, as shown in Table 7.2. For instance, the personality traits from the ‘OCEAN’ construct and the security scenario associated with each of the ‘OCEAN’ risk elements are combined to obtain cross-level interactions for the intention to commit computer abuse, as described in [116]. Then a weighted value is assigned to each personality trait, based on the security risk associated with each personality type, as described in the previous section 7.2. This step is then repeated for behavioural and technical risk indicators, such that, risk elements (Re) from each risk domain have corresponding weights (ReW), as shown in Table 7.2.

Domain		Risk Factors				
p_{risk-i}	R_e	O	C	E	A	N
	R_{eW}	0.35	0.21	0.45	0.25	0.65
b_{risk-i}	R_e	DB	IC	SV	DAA	IS
	R_{eW}	0.38	0.43	0.32	0.45	0.28
t_{risk-i}	R_e	UL	VRL	USI	FDM	VM
	R_{eW}	0.28	0.36	0.38	0.32	0.25

Table 7.2. Risk Elements

To determine the security risk status for an employee and decide if such an employee constitute insider risk to an organisation, consider the high-level algorithm for the malicious insider threat detection in Table 7.3. Firstly, organisations decide the value of $R.T$ for an employee, which is the number corresponding to the acceptable risk baseline for that employee. Each of the risk domains, i.e. personality risk indicators (p_{risk-i}), technical risk indicators (t_{risk-i}) and behavioural risk indicators (b_{risk-i}) have associated risk elements R_e . The input to the model has combined R_e from each of the p_{risk-i} , b_{risk-i} and t_{risk-i} domains. However, each R_e has associated and predetermined weighting factor R_{eW} . Also, each employee has a state for a given period with respect to R_e , such that; if the state of R_e is TRUE, the corresponding value for R_{eW} is returned. The output from the model is a numeric value $R.S$. For a given period, $R.S$ is obtained by aggregating all the R_{eW} for that employee. If $R.S$ is greater or equal to the $R.T$ that has been set for that employee, then it is assumed that insider threat activity is detected. Therefore, the employee is flagged for further investigation. Otherwise, routine monitoring would continue until there is a threat detection.

Algorithm

Personality risk indicators = p_{risk-i}

Behavioural risk indicators = b_{risk-i}

Technical risk indicators = t_{risk-i}

Risk-threshold (R.T) = acceptable baseline allowed for an employee.

Risk Score (R.S)

Risk Elements = R_e

Risk Element Weights = R_{ew}

STEP 1: FOR each EMPLOYEE:

There is an input (p_{risk-i} , b_{risk-i} , t_{risk-i});

There is an output (R.S);

To determine R.S for an EMPLOYEE:

Organisation decide values for R.T: 1.55

Make a list of all possible $R_e = \{r_1, r_2, r_3, \dots, r_n\}$

Make a list of corresponding $R_{ew} = \{w_1, w_2, w_3, \dots, w_n\}$

There is a STATE = TRUE, FALSE (1, 0)

Such that, in each month:

STEP 2: FOR each employee risk assessment (p_{risk-i} , b_{risk-i} , t_{risk-i})

IF the State for $R_e = 0$

Return (NULL)

IF the State for $R_e = 1$

Return (R_{ew});

$R.S = \sum(R_{ew})$;

IF $R.S \geq R.T$

Insider threat is detected;

Flag employee as malicious;

ELSE IF $R.S \neq R.T$

Return to STEP 1;

Table 7.3. High-Level Algorithm for the Malicious Insider Threat Detection

7.4 Simulation Result and Discussion

The preliminary simulation is done in MATLAB by using matrix tables for all true states of R_e and corresponding R_{ew} . Simulation output of our model is shown in Figure 7.2. As independent variables change over the 12-month period, the user risk profile is shown as the sum of the R_{ew} from the three risk indicators that are associated with that user, for each time period.

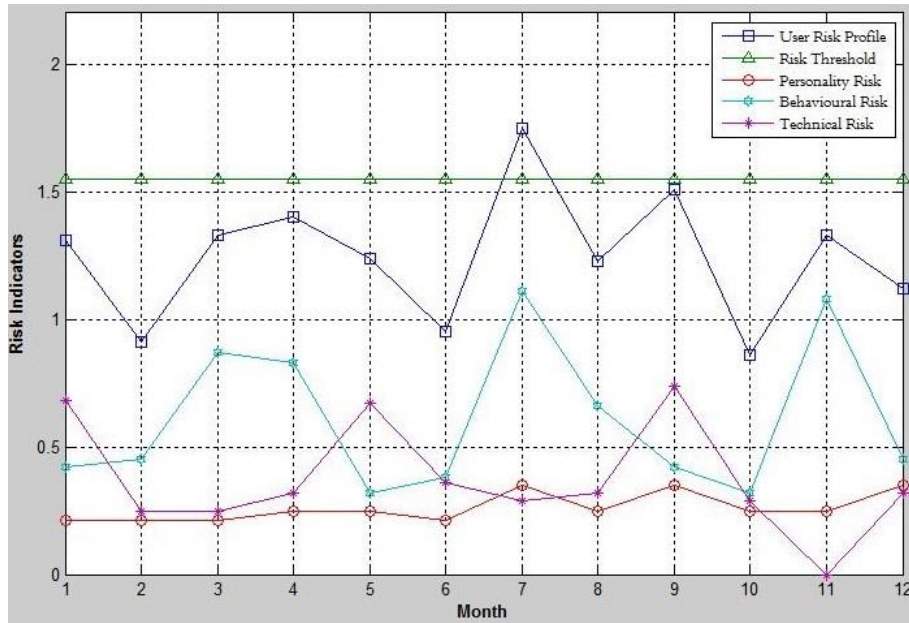


Figure 7.2. Simulation output showing how to detect malicious insider activities from multiple risk indicators

For illustrative purposes, the R.T for the employee under consideration is set at 1.55. In month 7, the user risk profile is above the R.T value of 1.55, set for that user; indicating that insider threat is detected, and the user is flagged as malicious. In month 7, personality trait 'O' is recorded for the user based on a chosen profiling method. HR records 3 or more counts of 'DAA', 2 or more counts of 'DB' and 4 or more counts of 'IS'. Similarly, IT security record shows 2 or more counts of 'VRL'. By aggregating all the risk indicators and comparing R.S to the user's R.T, it shows early warnings of malicious insider activities. Crucially though, treating each of the threat indicators in isolation is not enough to trigger the user as malicious, even though there may be false positive indicators in some cases. Consider month 11, HR b_{risk-i} record for the same user has a risk indicator value of 1.11; this value is quite a negligible

difference to the record for month 7, which has a b_{risk-i} value of 1.09. However, the IT t_{risk-i} recorded in month 11 has a risk indicator value of zero, this is significantly different from the record for month 7, which has a risk indicator value of 0.36. The p_{risk-i} for month 11 and month 7 is also similar, at risk indicator values of 0.25 and 0.35 respectively. Therefore, if the user is assessed based on b_{risk-i} alone, activities for month 7 and 11 would be flagged, which could trigger a false positive alert. However, combining all threat indicators from different domains shows a significant difference in the user's activities for both months, and only the activity of month 7 exceeds R.T.

The result from this model relates to the second research question on the importance of risk aggregation from unrelated domains in order to safeguard against cyber risk protocol violations. Importantly too, the model also complements the attributes of the system dynamics model discussed in Chapter 5. Thereby, suggesting that all the associative properties of employee behaviour discussed therein are required for malicious insider activities detection. This result also challenges the study in [104], in the sense that personality traits of individuals and efficacy factors alone are not strong enough for a conclusive and categorical prediction of employees' violation of security protocol. This assertion is also supported by the study in [245], which argues that individuals can manifest different personalities to a different degree depending on what is at stake. This study, therefore, concludes that risk aggregation from a wider domain, including what is proposed in [104] is a better approach to insider threat detection.

7.5 Conclusion

The starting point for managing organisation risk is the insider threat assessment, upon which management can build extra layers of controls like policy guidelines, awareness training and technical security solutions. Behaviour analytics is just one more tool in the arsenal of security analysts that can be deployed to support policies with the aim to get more secure. Taking something basic like web surfing as an example, if an organisation has a policy that banned employees from visiting certain websites sites during business

hours and those sites are not blocked; then the employees have to be trusted not to violate that policy. In order to ensure that employees adhere to the policy, it must be enforced; because a policy that can't be enforced is just a piece of paper. The enforcement is more likely to be in the form of technical tools observable from the IT perspective. The policy, however, gives the administrative control that is observable from the HR perspective. Policies can then be enforced based on individual employee risk profile supported by detectable behavioural patterns that are obtained from both IT and HR. Employees don't just turn up to do bad things; they also don't suddenly become security conscious either, most of the time, employee behaviour reflects what they do when not at work. It is the organisation's responsibility to ensure that businesses are protected from employees that intentionally or unintentionally violate security protocols.

This chapter proposes an approach that can get valuable insight into the activities of malicious insider so that organisations can have more information to draw inferences about insider actions during an investigation. This work describes an analytical model that considers risk elements from different risk domains, such that when each domain is treated in isolation, it may lead to insufficient evidence of malicious intent. However, when the intersection of different risk indicators is considered as a single block, it offers a considerable improvement in the possibility to detect an insider threat. The results in this chapter have been explained with reference to theories and past literature, and we suggest that future research examines the relationship and critical attributes that specifically link evidence of malicious intentions from technical log information, human behaviour and personality traits.

This model has significant implication for security professionals, to draw insight from inextricably linked risk domains within the context of cybersecurity management. However, substantial empirical work is still needed to evaluate the model in real-world cases, like banking organisations. Also, the model could be useful to order highly significant developing insider threats that require security analysts' review and could also provide further insights into collective management of information security in organisations.

8 INCENTIVES AND SECURITY INVESTMENT DECISIONS IN INFORMATION SECURITY

"If you spend more on coffee than on IT security, you will be hacked.

What's more, you deserve to be hacked."

-White House Cybersecurity Advisor, Richard Clarke

"This chapter has been published in Fagade, T., Maraslis, K. and Tryfonas, T. (2017) 'Towards Effective Cybersecurity Resource Allocation: The Monte-Carlo Predictive Modelling Approach', International Journal of Critical Infrastructures, 13(2/3), p. 152. doi: 10.1504/IJCIS.2017.088235. The paper was rectified by Dr Theo Tryfonas."

8.1 Introduction

The overall process of information security risk management is all-encompassing, from risk identification to business impact and risk reduction decision [249]. Organisations invest in technical and procedural capabilities to ensure the confidentiality, integrity and availability of information assets and sustain business continuity at all times. However, it is useful sometimes to express the cost of security as the economic activity function relative to the core business of an organisation, even, the key quantity of investment theory is expressed as a cost-benefit ratio of investment, regarding the production function and the amount of output per unit input [250]. This is also applicable in the context of information security domain, where security investment models are built on parametric variables defined as inputs and outputs [154]. When information security system is evaluated from an economics perspective, it becomes apparent just how little metrics can be obtained from technical explanations to satisfy the questions of how “much should be allocated for security investment?” Or “What is the adequate level of security?” [251]; because optimal resource allocation for security is often affected by intrinsically uncertain variables, leading to disparities in resource allocation decisions.

In light of the literature review of the resource allocation problem discussed in chapter 2, this study explores how the Monte-Carlo simulation model can be applied to efficient cybersecurity resource allocation. It investigates how to make a business case for budgeting decisions within a conceptual enterprise/SMBs. Monte-Carlo simulations have been extensively used by risk analysts in various fields of study to make future risk estimations [252]. This is a popular method in different research domains like engineering, medicine, economics, biology and management finance [253]. It introduces randomness and simplifies computational complexity in the design, implementation and evaluation stages of theoretical models to estimate uncertainties [254]. Monte-Carlo simulation can perform quantitative risk analysis by assigning a probability distribution to uncertain parameters; and through random sampling of the distribution, it is possible to determine all

potential outcomes under those uncertainties [137]. In this study, Monte-Carlo simulation is applied to uncertain model variables like the impact cost of a breach to various information assets; in order to arrive at appropriate resource allocation in support of security investment decision for those assets.

The structure of the rest of this chapter is as follows; risk management overview is presented in section 8.2. The background description of our predictive modelling approach is covered in section 8.3. Model assumptions, scenario and methodology, are covered in section 8.4. Results and discussion are covered in section 8.5. Conclusion and future work implications are covered in section 8.6.

8.2 Risk Management Overview

Information security risks are generally described under the broad categorisation of disaster or abuse. The top priority of chief information security officers (CISO) and management are to ensure continuous functionality of IT resources at critical levels of operations [255]. Risk management can be described as a systematic and logical approach to identifying, treating, analysing and monitoring risks in any process [256]. Managers benefit from risk management strategies because it has a direct bearing on how available resources are put to best use. Risk management is practised in both private and public sectors; including healthcare, government establishments, insurance, finance and investments. However, in the context of information security, risk management is about the protection of information assets. Information security risk management is defined [255] as the protection of information assets from a wide range of threats in order to ensure business continuity, manage business risk and maximise return on investment. Risk management within the context of an organisation involves the implementation of appropriate controls to mitigate, share, transfer, insure, accept and continually manage risks as set out in the ISO/IEC Standard [18]. The ISO/IEC2700 series of standards define best practices, baseline requirements and controls for information security management systems (ISMS), under the confidentiality, integrity and availability (CIA) triad. In

addition, given that threat climate changes all the time, an essential element of the risk management cycle [256], is that the effectiveness of security controls be periodically reappraised by organisations. There are various reasons why an organisation may require some measures of security control against potential threats; these could stem from internal factors like corporate regulations and organisational policies or mandatory external influences like the data protection acts or compliance requirements of industry regulators [15]. Whatever the driver, it is apparent that risk management will involve some mitigation control investments and resource allocation decisions.

However, information security professionals often do not quantify and communicate risks effectively in order to attract the right level of resource allocation. Organisations may struggle to present a measure of accurate cost benefits of information security activities, primarily because, security investment results in loss prevention rather than profit margins [257]. Also, business executives often opt for compliant security, whereby, baseline requirements of standards like the ISO2700, NIST or other guidelines are implemented, then businesses operate under the assumption that compliance equates security. The costs associated with risk management range from personnel to hardware and software outgoings. Therefore, information security expenditure is a crucial resource allocation decision, yet little is known about the budgeting process used to ensure optimal investment in information security capabilities [258], or at best, the budgeting process is generally beclouded with ambiguities.

Traditionally, organisations use risk assessment model to determine the optimal allocation of resources to cyber capabilities. This approach is a flavour of risk-based regulation whereby firms determine their security investment based on risk assessment, potential losses and investment profile [259]. An organisation's budgetary decision is then based on a risk scoring matrix and its threat tolerance, given the score value. Risk scoring matrix is calculated on the assumption that an event will happen given a probability of occurrence and impact or severity of security breaches. Information security

budget is then allocated based on the resultant estimated risk score. The risk scoring formula is given as:

$$\text{Risk} = \text{Probability(P)} \times \text{Impact(I)}$$

The value of (P) and (I) for a given asset is assigned based on expert opinion, the statistics from reports, corporate level assessment or records from past events and the resultant single value represents the risk score for that particular asset. To suggest that the risk impact to information assets are subjective probability estimates is somewhat ambiguous and deterministic [148]. In practice, it is difficult to apply this calculation to real-world problems, in order to optimise resource allocation decisions. This approach raises the question of reliability [260], as risk predictions are misrepresented for effective mitigation. Information security risk and management is transitory; hence, the actual impact of risky events might not be an accurate reflection of the current deterministic estimation.

8.3 A Background Description of our Predictive Model

8.3.1 Different Approaches to Resource Allocation Decision Processes

When risk analysis is based on the traditional risk matrix approach, security assessors extrapolate that under certain assumptions, specific events would be true; while entirely discarding the possibility of least significant and extreme events as part of that extrapolation.

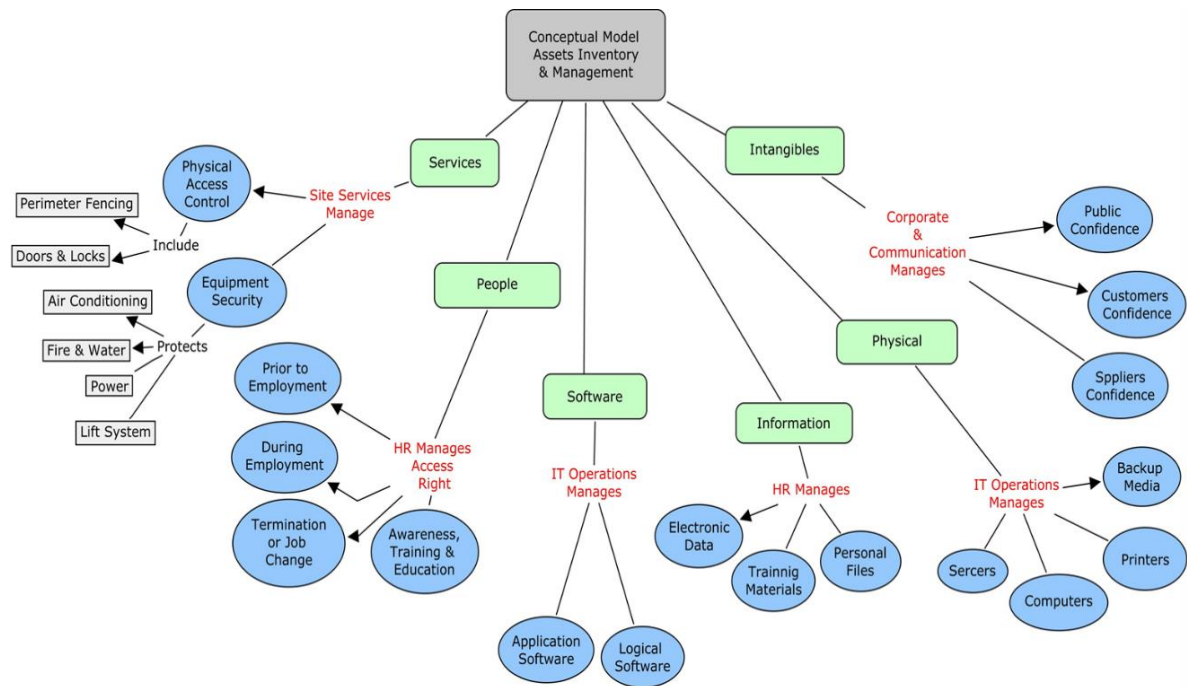


Figure 8.1. High-level conceptual model diagram

For organisations that base its threat tolerance on information security risk assessment, trying to guess the odd under so many uncertainties can only lead to erroneous results. The difficulty of this approach is further emphasised in [261], where it is stated that the efficient allocation of resources under the circumstance of uncertain risk and severity of breach cost is very hard. In order to explain how uncertainty affects security breach costs and resource allocation decision to mitigate those risks, this study presents a high-level and low-level conceptual enterprise scenario for a bank in Figure 8.1 and Figure 8.2 respectively.

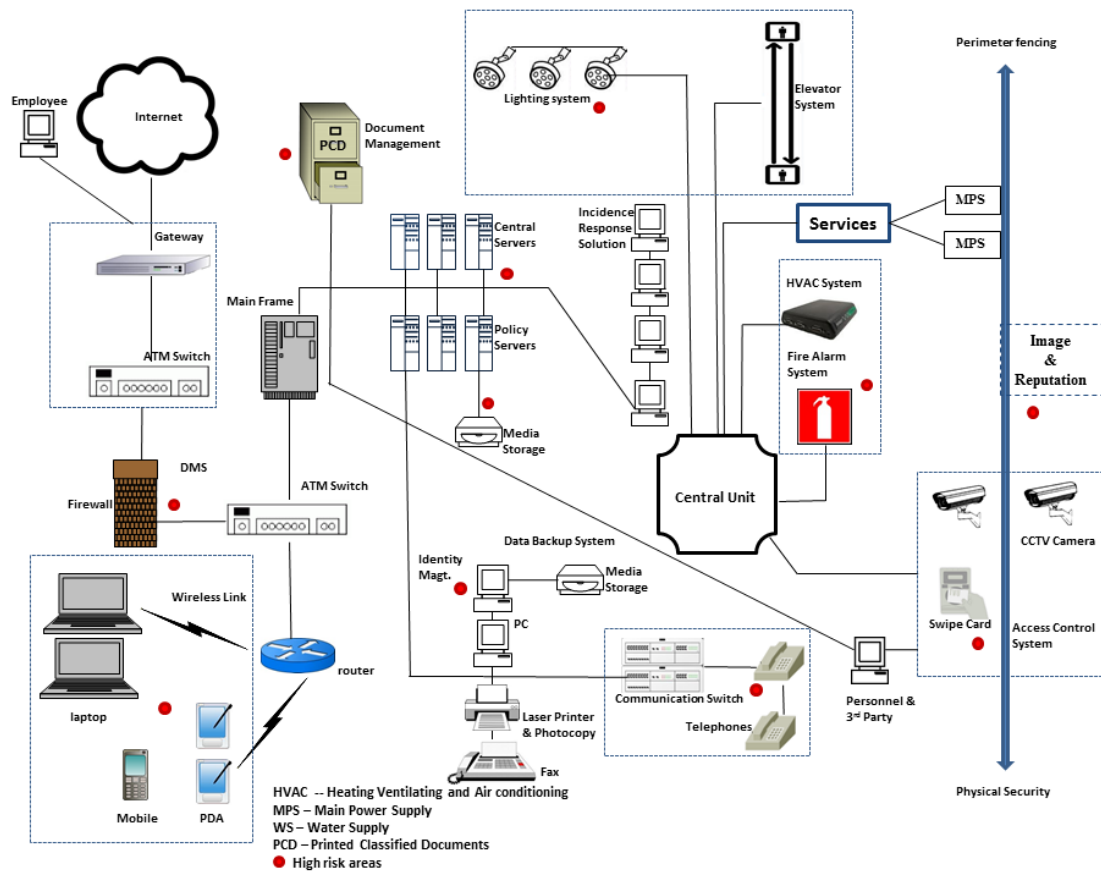


Figure 8.2. Low-level conceptual model diagram showing key asset points

We assume that the bank only has five high-risk asset points that need to be safeguarded from security threats at all times. Also, stakeholders' resource allocation decision is based on the severity of the breach of those assets and how it may impact banking operation. The reason for this assumption is to focus on only five hypothetical high-risk assets and to minimise the complexity of our simulation at this stage. For illustrative purposes, we consider DDoS mitigation system, personnel and third-party contractors, data backup and recovery system, incident response solution, and antivirus software as the key asset.

8.3.2 Deterministic Estimation of Security Breach Costs

Likelihood	Description	Frequency of Occurrences
1	An incident is expected to occur in exceptional circumstances, e.g. once in 10 years	Rare/Very Low
2	An incident may occur at some point, e.g. once in 3 years	Possible/Low
3	An incident will occasionally recur, e.g. once in a year	Probable/Medium
4	An incident will occur in most circumstances, e.g. once every 4 months	Certain/High
5	An incident is certain to occur in most circumstances, e.g. once every month	Frequent/Very High

Severity	Description	Example of Business Impact
1	None: no disruption of service	Financial loss < £1000
2	Minor	Financial loss < £10, 000
5	Moderate	Financial loss < £100, 000
10	Significant	Financial loss < £1, 000 000
15	High	Financial loss > £1, 000 000

Table 8.1. Risk likelihood and severity

This approach is based on the use of conventional risk assessment model to determine appropriate resource allocation. Deterministic point estimation is associated with random variability like a game of chance. In a roll of a die, probabilistically, there is a 1/6 chance that a certain number would come up, and it would have an interpretation given long-term frequency. Risk/vulnerability output based on five scale levels of very low, low, medium, high and very high also have the same element of chance, whereby risk ratings are assigned on a deterministic chance of occurrence. This is captured in Table 8.1 showing the description of the likelihood and severity of risk for critical assets, especially in terms of financial impact. Likelihood of risk is ranked on the scale of 1 to 5, where 1 is rare or very low, and 5 is frequent or very high.

Similarly, Table 8.2 shows the risk scoring matrix by taking into account the likelihood and severity value of each risk. Risk scoring is carried out by applying a simple multiplication process whereby the likelihood of risk is multiplied by the severity of that risk occurring. The risk rating is then applied after scoring each risk, by choosing the most appropriate definition under likelihood and the most appropriate definition under severity. This is achieved simply by looking up and matching the numbers on the risk matrix table to obtain the risk ratings. After the risk analysis phase, given an organisation risk threshold and the risk score number, security budget is then allocated for the countermeasures to mitigate risks in that context. The idea of risk assessment is to evaluate scenarios of security incidents and take proactive measure before it happens. Consider one of our scenario high-risk assets; a dedicated DDoS Mitigation System (DMS) that can deter DDoS attacks. How effective the DMS is to mitigate volumetric attacks may be uncertain, but it is unlikely that enterprise operations and vital computing resources will be subjected to complex layer 7 attacks, in order to ascertain if the defence mechanism is worthy of investment. Rather, it is more likely that historical data is used to assist with resource allocation decisions, but in the absence of data, estimations could be used. A risk analyst may make a statement that the probability of a successful attack without mitigation (the DMS) is three, and the impact cost is (\$53,477).

However, when deterministic point estimate is used to score risk and model uncertainties; what that actually means is that based on the subjective estimates for each asset point, the total breach cost without security for all tangible and intangible assets in the enterprise will always be the sum of breach costs to each asset [260], as shown in Table 8.3. If it is certain that an expert's deterministic estimate is 100% reliable, then the potential cost of a security breach should be fine. Hence resource allocation to mitigate those risks should correctly reflect the assessment.

Risk Rating Table – Likelihood x Severity					
Severity → Likelihood ↓	None	Minor	Moderate	Significant	High
	1	2	5	10	15
Frequent 5	5	10	25	50	75
Certain 4	4	8	20	40	60
Probable 3	3	6	15	30	45
Possible 2	2	4	10	20	30
Rare 1	1	2	5	10	15

Table 8.2. Risk rating table

In reality, security breach to some asset will cost less with insignificant impact while some may result in massive losses with catastrophic consequences. Therefore, resource allocation under uncertain risk-based assessment is unlikely to match risk mitigation efforts [148].

Average annual cost of security breaches in the magnitude of \$K/year		
Assets	Security Incidents	C = Cost of breach
DMS	DDoS Attack	53,477
Personnel & 3 rd Party	Malicious Insider	40,403
Recovery System	Data Loss	39,905
Incidence Response	Cyber Espionage	69,026
Anti-Virus Software	Malicious Code Infection	31,572
Total		234,383

Table 8.3. Expert estimation of security breach costs

8.3.3 Probabilistic estimation of security breach costs

In order to address the high-level of uncertainties associated with the deterministic approach, especially in view of increasing information assets; risk analysts can consider probabilistic estimation approach. Through Monte-Carlo simulations, the probabilistic cost of a breach can be determined for each asset in a given scenario. The Monte-Carlo simulation works by sampling lots of scenarios from a probability distribution instead of static point estimates [137]. Probabilistic estimation assigns minimum and maximum cost boundaries for each security breach. The combined cost of all security breaches is then calculated as the total minimum and maximum cost of a security breach for each asset in order to project the total resource allocation for the enterprise. In that case, it is possible to establish absolute bounds for allocated resources to the entire enterprise. Monte-Carlo may not be able to tell with certainty the exact cost of a breach, but it can describe the probability of cost associated with security breaches, to aid resource allocation. In comparison to the deterministic approach, the probabilistic estimate is also based on random variables. However, each estimate follows a particular distribution, independent and unaffected by other variables.

Consider the deterministic cost of breach for the DMS as described in the previous subsection. Under probabilistic estimation approach, smearing out parameter can be used to suggest that in place of a fixed quantity like £53,477, the minimum value in of \$30,000 and the maximum value of \$65,000 can be included in a distribution, as shown in Table 8.4 . Essentially, a fixed value is replaced with a probability distribution, which is an accurate representation of the state in the real world. Hence, the fixed quantity is now our most likely value, but it is not the only possible value in the distribution. The key to Monte-Carlo simulation is that each variable is assigned a random value, and the total value is calculated thousands of times during the simulation. It, therefore, allows us to understand the risk that expectations may not match reality, and appropriate precautions can be taken [262]. It is difficult to compute values for multiple scenarios without some form of simulation [187], especially if multiple assets and security breach costs have to be factored in, as part of the

budgetary allocation process. Therefore, to reduce that complexity, the assets and scenario incidents considered for this study are limited to five.

Assets	Security Incidents	The unit cost of a security breach without risk mitigation investments (in the magnitude of \$K/year)		
		C_{min} minimum	= C_{ml} = most likely	C_{max} maximum
DDoS Mitigation System	Dos/DDoS Attack	30,000	53,477	65,000
Personnel and third-party contractors	Fraud/Malicious Insider	20,000	40,403	50,000
Data Backup and Recovery System	Data loss/Stolen Devices	25,000	39,905	45,000
Incident Response Solution	Cyber Espionage	35,000	69,026	75,000
Antivirus Software	Malicious Code Infection	15,000	31,572	37,000
Total		123,000	234,383	272,000

Table 8.4 Model simulation parameters

8.4 Methodology

There are two underlying assumptions for this model:

- Key information asset points are determined by an organisation CIO and the security team.
- Minimum and maximum values of security breach costs are subject to expert elicitation, based on experience and previous security breach events.

The work described in this chapter use some security breach cost parametric values obtained from verifiable information security breach reports. Model parameters are taken from the cost of a security breach report [263], and IT security risks special report series [264]. The study in [263] covered data breach cost and impact of 350 organisations around the globe. The study uses

activity-based costing (ABC) for data breach calculation which takes into account; direct cost, indirect cost and opportunity cost. It also takes into account a range of expenditure associated with organisation data breach detection, containment, response and remediation. The study in [264] covers corporate IT security risks survey of more than 5,500 companies in 26 countries around the world. It covers IT threats and the cost of recovery when a security breach occurs. Values taken from both studies serve as input parameters for our simulation model as shown in Table 8.4. **Error! Reference source not found.** However, limitations of the costing methodology outlined in the studies are not validated nor described in this work.

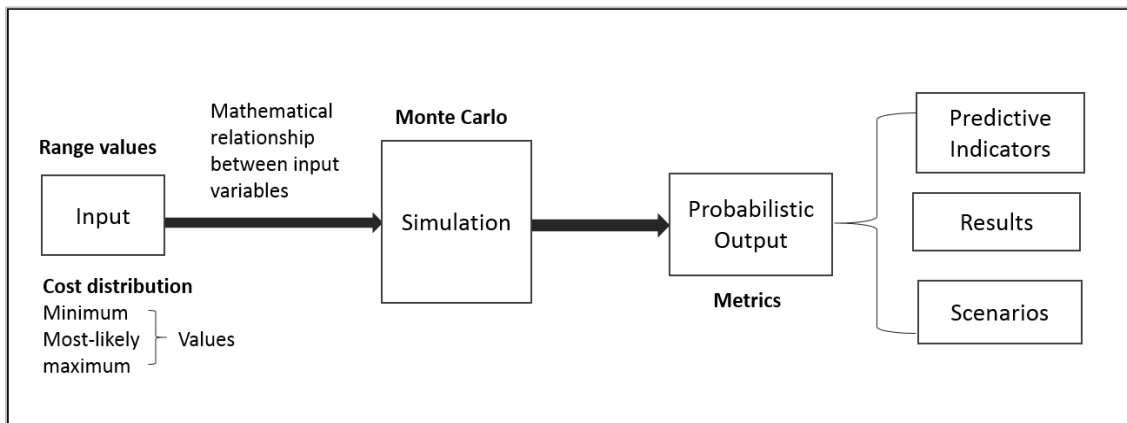


Figure 8.3. Schema of the MC predictive model

We identify uncertain deterministic security breach costs in our model and convert them into a range of values using a triangle distribution, as shown in Figure 8.3. For each breach cost estimate, given an asset, fixed values are replaced with a probability distribution. Triangular distribution used in this model is one of the most used probability distributions to elicit expert opinion, especially in the case of limited or absence of historical data [137]. It defines uncertain breach cost values as a minimum (C_{min}), most-likely (C_{ml}) and maximum (C_{max}) range of values, for each asset in the model calculations.

This approach follows the model implemented in [168], whereby the (C_{min}) and (C_{max}) are held constant while the (C_{ml}) is selected randomly from the distribution graph. (C_{ml}) are non-negative random variables which follow

a triangle distribution. For this simulation, MATLAB and Vose ModelRisk software [265] are utilised, both tools allow configurable simulations with a vast number of runs and can generate thousands of scenarios for each set of uncertain inputs. ModelRisk uses a mathematical model for input variables and triangle distribution function given as:

$$f(x) = \frac{2(x - C_{min})}{(C_{ml} - C_{min})(C_{max} - C_{min})} \quad \text{for } C_{min} \leq x \leq C_{ml}$$

$$f(x) = \frac{2(C_{max} - x)}{(C_{max} - C_{ml})(C_{max} - C_{min})} \quad \text{for } C_{ml} \leq x \leq C_{max}$$

The simulated output is generated given the mathematical relationship with input variables, and the results provide predictive indicators to support decision-making processes. However, with Monte Carlo, input variables for the simulation model are uncertain, random and defined according to a probability distribution in order to capture and model those uncertainties. In this model, what happens is that thousands of scenarios are generated to reflect a probabilistic output for each uncertain input, according to triangle distribution, then, the resultant output values are computed thousands of times over again during the simulation. However, in order to obtain a convergence and more realistic values, a recommended run of 10000 simulations is required, and 1000 iterations are the barest minimum acceptable [266]. We generate 50000 simulation runs; the model output is a probabilistic range of values and scenarios associated with security breach costs, as well as the probability distribution associated with those values.

8.5 Simulation Result and Discussion

Results of the Monte-Carlo simulation shown in Figure 8.4 add an extra dimension to the initial deterministic values. As the simulation begins, samples are taken from each of the security breach cost probability distribution. ModelRisk then computes the average random value at the end of each iteration. During the simulation, different scenarios are generated based on the frequency proportional to the probability of those scenarios occurring.

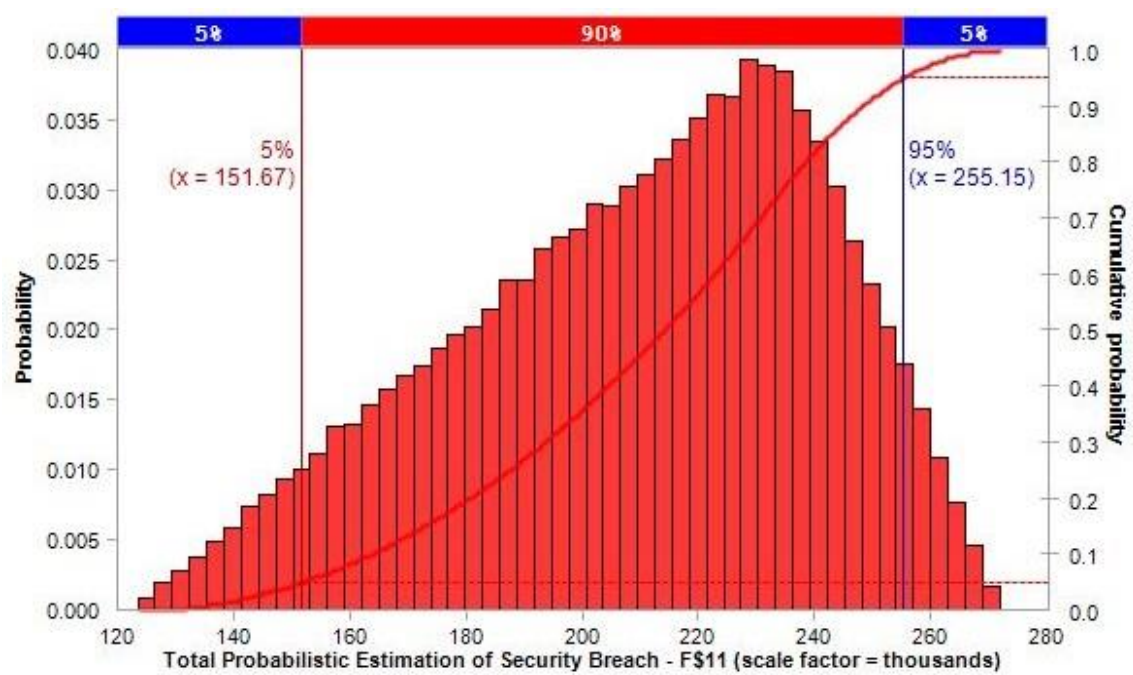


Figure 8.4. Simulation result in 'ModelRisk' with cumulative overlay

At the end of the simulation, the output histogram represents 50,000 scenarios for security breach cost. The result of the simulation takes into account all uncertainties, and it is in the form of probability distribution similar to the input parameters. These distributions represent possible outcomes, rather than single point predicted outcome.

From the model result in Figure 8.4, it can be seen that the upper 5% and the lower 5% represents extreme cases that are ignored by the simulation output. From the parametric values in Table 8.4, it can be seen that the total resource allocation could be as low as \$123K or as high as \$272K, but the realistic chance of resource allocation nearing these extreme values is very

unlikely. Hence the model ignored them. It can be seen that 90% of the simulation iterations fall under a value less than the upper bound estimated total values. Hence, we can say that 90% of the total allocation will meet our initial estimate. While this is not a guarantee, it allows us to adjust IT security budget to match the cost of potential breaches and also understand the risk that resource allocation may not meet initial estimates.

Further analysis of the result in Figure 8.4 shows that given all the iteration of simulations, the absolute minimum value of \$151.67 is much higher than the original deterministic lower bound value of \$123k. Similarly, the absolute maximum probabilistic value of \$255.15k after iteration is much lower than the deterministic value of \$272k, with only 5% chance of the allocation going over the upper boundary.

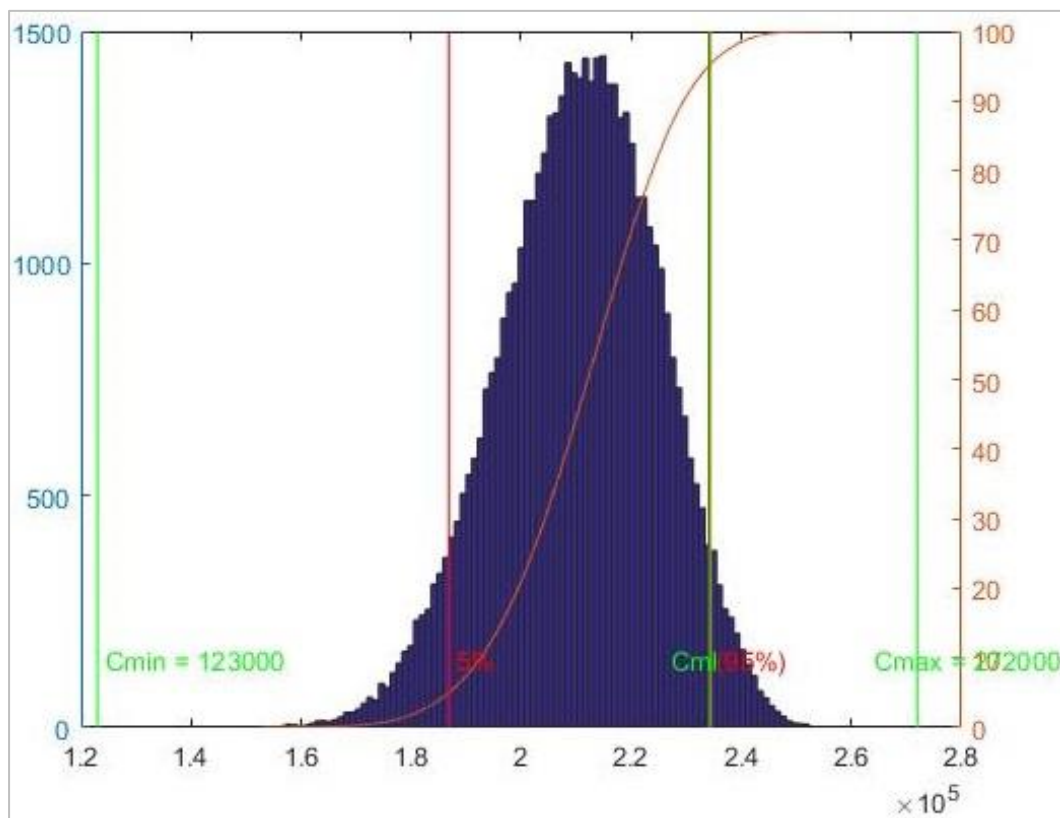


Figure 8.5. Simulation result in MATLAB showing values for C_{min} and C_{max}

The most likely point estimate is around the value of \$229k; from the location of the peak of the distribution, it can be seen that this value is somewhat more realistic than the deterministic value of 234,383. However, the cost of impact

could be significantly higher, possibly twice as high in terms of cumulative percentage or frequency distribution.

In an attempt to validate our model, the result is compared with another simulation in MATLAB shown in Figure 8.5, using the same input parametric values. The invariant that holds in both states of the models is that extreme values are ignored in the output of both simulations. While both models follow a similar distribution, it can be seen that not only did both simulations ignore lower and upper bound values, but also shows higher C_{\min} and lower C_{\max} than the deterministic values. This also confirms the correctness of the representation entities and the model behaviour.

8.6 Conclusion

Many businesses have been obliterated as a direct consequence of security breach, leading to substantial economic impact and in most cases loss of intellectual assets to cybercriminals. In order to defend against cyber threats, organisations invest in countermeasures, to protect processes, people and information assets. However, deliberate evaluation of optimal resources for countermeasure investment is often hindered by intrinsic variables. This study explored how Monte-Carlo predictive simulation model can be used within the context of information technology to reduce these disparities. Using a conceptual enterprise as a case study and verifiable historical cost of security breaches as parametric values, our model shows why using conventional risk assessment approach as budgeting process can result in significant over/under allocation of resources for cyber capabilities.

In general, predictive models allow us to make more useful and less erroneous decisions. Making important decisions without diligent consideration of uncertainties in the budgeting process can lead to unrealistic values. Forecasting with accuracy, on how much damage a successful security breach can cause is a real challenge for risk managers, especially when multiple assets and associated threat exposure are considered. Again, three-point estimates, for all assets tend to become unreliable as the complexity of asset classes in the model increases. Using probabilistic simulation, therefore,

simplifies the complexity of cost estimation processes. The application of Monte-Carlo simulation to security investment decision, in particular, allows us to visualise different probabilistic outcomes in view of what might go wrong; given best case, worst case and most likely case scenarios.

MC allows us to understand the outcome of scenarios and help to understand unexpected pattern without necessarily exposing information assets to real threats. The output of Monte-Carlo simulation is a range of values and risk assessor can derive confidence level from that range. It is expected that predictive models will enable management to make more effective decisions and be part of the analytical input for policy formation. If there is a sound understanding of what might go wrong, decision makers can utilise the model to implements appropriate risk mitigation strategies and budget allocation for security investment. This chapter will be expanded as part of future work to include resource allocation for different information assets. A model that breaks down security budgets into fragments for further allocation, such that, information assets with the highest frequency and impact of threat events are allocated more resources than those with low impact events.

SECTION 3: CONCLUSIONS AND SUGGESTIONS FOR FUTURE WORK

In this section, the research findings of this work are presented along with the ideas for future work.

- Chapter 9: Research Findings and Future Work

9 RESEARCH FINDINGS AND FUTURE WORK

"I am a slow walker, but I never walk backwards."

-Abraham Lincoln

This chapter sums up the thesis and presents the research contribution to the body of knowledge, especially the information security management research community. The work in this thesis covers exploratory studies, model developments and suggests alternative approaches to the management of information security problems. Some of the outputs from this research have been published in conferences and journals publication as indicated in the list of publications. Finally, this chapter concludes with the research implications for academia, limitations and possible areas of extension as part of future work.

9.1 Conclusion

Following an extensive literature review of academic articles, this thesis identifies gaps in three specific areas of information security management for organisations. The gaps identified suggests that there are some inadequacies in the current approach to risk management in the areas of compliant security, insider threat mitigation and resource allocation for security investment. The literature gaps have also lead to the research questions, to which this study have presented concepts and methodologies to answer each question.

The compliance-based solution for ISMS is conformity to security requirement, but it does not mean that an organisation is secured in the actual sense. The general notion of compliant security is that organisations can defend security adequacy through compliant consistency. For instance, in the event that an organization is security focused rather than compliance and a security breach occur; it is not as easy to justify the organisation's security efforts, regardless of whether the organization has a substantially more grounded security program set up. If compliance is evaluated against security, the assumption is that compliance is substantially less demanding to quantify, but easier to justify in the event of a security breach. This dynamic has led to a situation where many organisations opt for security through compliance, even if the heightened sense of security that compliance sometimes present may not be in the best interest of the organization at the long run. The prominent challenge to organisations' compliance programs is the employees, whose malicious or inadvertent actions could lead to the violation of security protocols.

Malicious insider activities are difficult to lock down, given that insiders already reside behind organisations firewall. Insiders also constitute the most expensive form of security breach, and the trend is set to increase significantly, despite organisations spending a fortune on security tools and guidelines. In banking and financial organisations, the complexity of the operating environment is tied to critical information assets and business processes such that when adversaries carry out attacks, the effect often has a colossal impact on organisations in terms of the loss of time, capital gain,

human resources, reputation and competitive advantage. However, in line with previous literature on the connections between cybersecurity conventions, security protocols violation and how employees rationalise and defend security behaviour. The study examines how this knowledge can be explored to model and analyse a scenario for the prediction of malicious insider activities.

In terms of security budget, cybersecurity is one of the most significant difficulties confronting business organisations in the modern days. Although, when an organization operates on the small or medium scale, threat exposure is still imminent, it is comparatively easier to maintain and assign resources for information security investment. However, when IT budget is constrained, as organization scales up and the number of assets to be protected grows; there would be a point where a deliberate evaluation of information security investments will be needed to defend against the threats to information assets. Organisations invest in countermeasures to mitigate risk exposures and prevent events that could undermine the confidentiality, integrity and availability of mission-critical systems. However, security resource allocation process is subjective and appeals to the risk appetite of key stakeholders in different ways. Therefore, optimal resource allocation to security is often affected by intrinsically uncertain variables that can lead to disparities in resource allocation decisions. This study explores how Monte-Carlo predictive simulation model can be used within the context of information technology to reduce these disparities and aid security investment decisions, through a single block optimal resource allocation.

In conclusion, this study acknowledges that risk management is an ongoing game between security managers and adversaries who are either consciously or unwittingly violating security protocol. Through targeted training and information security culture, organisations can use policy-based segmentation to protect network infrastructure, such that policies dynamically control access. By starting with security policies, employees can be monitored for early signs of malicious activities through profiling, whereby individual users have different roles in different environmental context.

System users are part of organisations security problems and not necessarily the solution, as such; users should be given just the right level of access to perform their job roles. By using policy to define security and profile employees, then embedding security in organisation culture, users can only access the applications they are authorised to use, wherever they are, even if all the applications are bundled together in one place. If employees are profiled based on work schedules and authorised system interactions, and if the number of assets they can have access to is restricted to individual job functions. Then, organisations can limit the number of damages that can be caused by lateral movement, server exploitation, malware and so on. Even when employees can outstep their boundaries, the intention to violate security protocols can be captured when the variation (of risk indicators) from other domains are aggregated.

9.2 Findings

The findings from chapter 4 and chapter 5 are the response to the research question 1. The study findings suggest that compliant security is not adequate as a holistic protection model for organisation information assets, primarily because of how employees rationalise security behaviour. While this is not a new discovery, the study shows that the problem is valid and it still exists. Importantly, the findings from both chapters 1 and 2 are that employees disregard the consequences of their behaviour either because of the effect of efficacy factors on personality traits or the effect of 'Blaming the Victim' and 'Denial of Injury' on neutralization technique, as these effects are strong/significant on the intention to violate security protocol. This observation is also in line with the study in [267], which suggests that positive benefits are the primary consideration of employees that violate security protocols, rather than the negative consequences like sanctions. The piece of work discussed in response to the research questions one as follows:

- The application of quantitative analysis of survey data obtained from banking organisations to explore the viability of a compliant security model, as a regional case study (see in chapter 4). It also covers how relevant theories help explain the quantitative analysis of the survey data.
- Extending the findings discussed in chapter 4 through the application of the Partial Least Square Structural Equation Modelling (PLS-SEM) to explain our results. The compliance survey data obtained from banking organisations and the application of neutralization theory to security scenarios are combined to form hypotheses on the effectiveness of compliance-based security (see chapter 5).

The study in chapter 6 and 7 are the response to the research question 2. The study explores the risk factors that can be associated with personality traits, behaviour and digital footprints to explain how multiple risk factors can serve as a precursor to security protocol violation. It is apparent that risk factors aggregated from unrelated domains are better predictors of the intention to violate IS security policies rather than when these factors are considered in isolation. Although while previous studies may have already established that depending on security scenario effects, certain personality traits have the propensity to violate security protocol than others. However, the current study also shows that while that may be true, other factors are as important as individual personality. The argument is that, while personality traits are fairly stable throughout an individual's lifetime, external factors that can trigger behavioural changes in individuals are equally important as personality profiling, in anticipation of a security violation. The piece of work discussed in response to the research questions two as follows:

- System Dynamic approach to the modelling of malicious insider activities. The model input utilises risk indicators from different domains to dynamically analyse the interplay between different risk factors and show how those interplay can increase the chance of cyber-security incidents in banking organisations (see chapter 6).

- The design of a conceptual model of malicious insider detection. The model aggregates the weighted values of different risk factors from unconnected domains and simulates the output using MATLAB. The result of the model can be used as part of the resources for managing organisation insider threat assessment. It can also be used to obtain insights about malicious insider activities to draw inference about insider action during security breach investigations (see chapter 7).

Chapter 8 is the response to the research question 3. The economic impact of the cyber breach is huge, but lack of readily available data to quantify the potential losses associated with cyber-attacks also makes it difficult to allocate the right level of resources for risk mitigation efforts. This problem space is addressed through a model of a single block resource allocation. The piece of work discussed in response to the research questions three as follows:

- The study applies a Monte-Carlo Simulation model for resource allocation and security investment. In particular, it shows how using “ModelRisk”, a risk analysis tool and a three-point probabilistic estimation of data breach costs, can simplify resource allocation for complex asset classes in an organisation (see chapter 8).

9.3 Contributions

The gaps identified in the literature guided this study to construct three research questions. In order to answer the research questions, this study utilised the Standards Publications ISO/IEC 27001 and other human behavioural theories to explore the viability of compliance as a security model in banking organisations. In particular, the study links one research question to the other, such that, the problem of information security management is addressed at three sub-element levels. The study is, therefore, able to accentuate the need for the following:

- To understand the real value of compliance for organisations from the perspectives of information security.
- A better understanding of how behavioural theories, criminology theories and personality dimensions can help manage security protocol violations in organisations.
- A better understanding of the malicious insider problems through the aggregation of risk factors from unrelated domains.
- A conceptual model for predicting malicious insider activities.
- A model for reducing discrepancies in resource allocation for security investment decisions.

Following the identified needs as itemised above, the study proceeds with the methodologies and model development that specifically addresses each need.

The study contributes to the body of knowledge and the research community by presenting different approaches to information security management in organisations while focusing on three sub-element areas. The research questions developed in this study and the specific contributions to knowledge as a consequence of that are summarised as follows:

“Is security by compliance adequate for the protection of organization information assets?”

- The study contributes to the research community by providing in-depth analysis of the viability of compliant security. It is one of the first studies in the context of information security management for Nigeria banking organisation, as part of a sector case study. It evaluates employee security compliance against the widely adopted ISO/IEC 27001 security standard and concludes that compliance often leads to a false or a heightened sense of security. The study then proposes how information security may be embedded into organisation security culture in that context.

“How can we profile malicious insiders by aggregating risk indicators from unrelated risk domains and safeguard security protocol violations?”

- The study also contributes to the body of knowledge by building on relevant theories in psychology, criminology, economics and behaviour to present a conceptual model for the prediction of malicious insider activities, through the aggregation of risk indicators from different risk domains. In particular, it proposes a multi-domain approach model as a benchmark for malicious insider threat detection, by aggregating feedback from personality traits, behavioural changes and technical log information to simulate the behaviour of an insider.

“How can we address the issue of misaligned incentives and improve resource allocation decisions for cybersecurity investments?”

- The third research question encapsulates the first two because it is based on resource allocation to manage information security initiatives. The challenges of resource allocation for the protection of organisation cybersecurity initiative is underpinned by the uncertainty in the budgeting process and the lack of ability to forecast with any accuracy, the impact of security breaches. In response to the third research question, the study also contributes to knowledge by presenting a Monte-Carlo Simulation model in support of resource allocation decision for security investment.

9.4 Limitations

It is important to reiterate that different elements in this study involve the use of models to explain our results. Models are important research tools that enable researchers to address complex real-world problems in abstraction; as such, even models that are based on poor data can be helpful to address phenomenon issues, if available data and expert judgement contribute to identifying important determinant structure [3]. The results of this study have shown that the models are reasonable and useful to explain behaviours and

processes, based on expert opinion, feedback from academic conferences and other stakeholders. Nonetheless, the work conducted in this thesis is not devoid of limitations. Some of the possible limitations identified are discussed as follows:

- This study is able to develop a valid scale for compliant security construct. However, the relationship of this construct to security management in banking organisations cannot be empirically tested in a wider spread of banking organisations. This study is limited to few banks in the two major cities of Nigeria (Lagos and Abuja) and did not include other regions of the country. Further research may be required to make this construct functional and perhaps more representative by increasing the sample size of the study. Banks in other regions of the country need to be considered as part of a wider case study, and perhaps improves the robustness of the sample data. Nevertheless, literature review indicates that there is a need to investigate the inappropriateness of compliant security, as the sole means of security management in organisations.
- The survey did not take other control variables into account like the size of the organization, age and education level of respondents which may lead to different statistical results when considered. Similarly, over 40% of the survey respondents work in Operations department of the banks, the way these employees interact with information systems may not be representative of how employees from other departments interact with information systems.
- In terms of other countries or sectors that are not banking or financial organisation specific, the research findings may not be generalisable, since compliance requirements and information security awareness varies across industries and sectors. The study may benefit from robustness by expanding the survey sample to include other non-banking sectors like private enterprises, NGOs and government agencies.

- The proposed models in this research require further empirical evaluation to validate the applicability of the models to insider problems and resource allocation decisions. Simulations and models, in general, have some limitations because they could sometimes lead to false representations. Models often involve assumptions which may or may not invalidate the result; whereas, real-world scenarios involve systems of infinite complexities which may not match those assumptions.
- Personality-based approach to profiling individuals may also have some limitations because depending on what people set to achieve, they can actually manifest different levels of personality, at different times and to a different degree [245]. Also, monitoring employees, especially when they are aware of being watched, they may become conscious of their actions, which may increase the stress level. In turn, this may trigger responses that could impact on security behaviour.

9.5 Directions for Future Work

In the light of information security management for organisations, the motivation, identified literature gaps and the research questions have been presented; and this thesis is able to address each question through a series of approaches. However, there are still areas of possible contributions as part of the directions for future work, hence, future research is suggested to include the following:

- More empirical studies are needed on the security by compliance model in organisations with the possibility of extending the study beyond banking organisations alone.
- As part of future work for the compliant security, the plan is to expand and test the validity of the observations in this study and also, suggest ways to integrate human-centric technical procedure into compliant security model.

- Develop a framework for a customizable cybersecurity training that is fit for different types of personality risk attributes.
- Application of the insider threat prediction model in a real-world enterprise environment and banking organisations, to empirically explore and further test the validity and sustainability of the model.
- Expand the resource allocation model to include the breakdown of security budgets into fragments for further allocation; such that, information assets with the highest frequency and impact of threat events are allocated more resources than low impact events
- A game theoretical approach to security investment decisions through experimental games whereby adversaries attack different organisation assets and defenders strategically chose from limited resources to invest in mitigating capabilities against the attacks.

REFERENCES

- [1] M. Belhocine, N. Zenati-Henda, S. Benbelkacem, A. Bellarbi, and M. Tadjine, "Integrating human-computer interaction and business practices for mixed reality systems design: a case study," *IET Softw.*, vol. 8, no. 2, pp. 86–101, Apr. 2014.
- [2] J. Hua and S. Bapna, "Who Can We Trust?: The Economic Impact of Insider Threats," *J. Glob. Inf. Technol. Manag.*, vol. 16, no. 4, pp. 47–67, 2013.
- [3] D. Andersen *et al.*, "Preliminary System Dynamics Maps of the Insider Cyber-threat Problem," in *Proceedings of the 22nd International Conference of the Systems Dynamics Society. Oxford, England.*, 2004, pp. 20–24.
- [4] D. Chinn, J. Kaplan, and A. Weinberg, "Risk and responsibility in a hyperconnected world: Implications for enterprises," *World Econ. Forum Collab. with McKinsey Co.*, no. January, pp. 1–40, 2014.
- [5] D. W. Straub and R. J. Welke, "Coping with Systems Risk: Security Planning Models for Management Decision Making," *MIS Q.*, vol. 22, no. 4, p. 441, Dec. 1998.
- [6] A. . "Ross, *Security Engineering: A Guide to Building Dependable Security Systems*. Wiley, New York, 2008.
- [7] L. . "Corriss, "Information security governance: integrating security into the organizational culture," in *"In: Proceedings of the 2010 Workshop on*

- Governance of Technology, Information and Policies*," 2010, pp. 35–41.
- [8] S. "Aurigemma and R. . Panko, "A composite framework for behavioral compliance with information security policies," in *"In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, "*, 2012, p. 3248–3257.
- [9] K. Renaud, W. . W. Goucher, K. "Renaud, and W. . W. Goucher, "The Curious Incidence of Security Breaches by Knowledgeable Employees and the Pivotal Role a of Security Culture," in *Human Aspects of Information Security, Privacy, and Trust*, Vol 8533., A. I. Tryfonas T., Ed. HAS 2014. LNCS: Springer, Cham, 2014, pp. 361–372.
- [10] M. "Siponen and A. . Vance, "Neutralization: new insights into the problem of employee systems security policy violations.," *MIS Q.*, vol. 34(3), pp. 487–502, 2010.
- [11] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "SECURQUAL: An Instrument for Evaluating the Effectiveness of Enterprise Information Security Programs," *J. Inf. Syst.*, vol. 30, no. 1, pp. 71–92, Mar. 2016.
- [12] L. Demetz and D. Bachlechner, "To invest or not to invest? assessing the economic viability of a policy and security configuration management tool," in *The Economics of Information Security and Privacy*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 25–47.
- [13] B. Srinidhi, J. Yan, and G. K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," *Decis. Support Syst.*, vol. 75, pp. 49–62, Jul. 2015.
- [14] G. Dhillon, "Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns," *Comput. Secur.*, vol. 20, no. 2, pp. 165–172, 2001.
- [15] Information Commisioners Office, "Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998," 2015.
- [16] B. Lee, "TalkTalk hack: Two men plead guilty to TalkTalk hack | IT PRO,"

2016. [Online]. Available:
<http://www.itpro.co.uk/security/24136/talktalk-hack-two-men-plead-guilty-to-talktalk-hack>. [Accessed: 23-Sep-2016].
- [17] G. Cluley, "Six months on from the TalkTalk hack - how has the firm suffered?," *Graham Cluley*, 2016. [Online]. Available:
<https://www.grahamcluley.com/talktalk-hack/>. [Accessed: 23-Sep-2016].
- [18] ISO/IEC 27001:2013, "BSI Standards Publication: Information Technology — Security Techniques — Information Security Management Systems — Requirements," Geneva, Switzerland, 2014.
- [19] BS7799-2:2002, "Information security management systems — Specification with guidance for use," London, 2002.
- [20] M. "Karjalainen, M. T. Siponen, P. Puhakainen, and S. . Sarker, "One size does not fit all: different cultures require different information systems security interventions," in *In: Proceedings 98 PACIS 2013*, 2013, p. 98.
- [21] I. Kirlappos, A. Beaument, and M. A. Sasse, "'Comply or die' is dead: Long live security-aware principal agents," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, vol. 7862 LNCS, pp. 70–82.
- [22] M. Theoharidou, S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799," *Comput. Secur.*, vol. 24, no. 6, pp. 472–484, Sep. 2005.
- [23] P. G. Neumann, "Insider Threats in Cyber Security," in *Advances in Information Security*, 2010, vol. 49, pp. 17–44.
- [24] F. L. Greitzer and R. E. Hohimer, "Modeling Human Behavior to Anticipate Insider Attacks," *J. Strateg. Secur.*, vol. 4, no. 2, pp. 25–48, 2011.
- [25] A. C. Johnston, M. Warkentin, M. McBride, and L. Carter, "Dispositional and situational factors: Influences on information security policy violations," *Eur. J. Inf. Syst.*, vol. 25, no. 3, pp. 231–251, May 2016.

- [26] R. Chinchani, D. Ha, A. Iyer, H. Q. Ngo, and S. Upadhyaya, "Insider Threat Assessment: Model, Analysis and Tool," in *Network Security*, Boston, MA: Springer US, 2010, pp. 143–174.
- [27] B. Schneier, "The psychology of security," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 5023 LNCS, pp. 50–79.
- [28] CBN, "Central Bank of Nigeria," 2015. [Online]. Available: <http://www.cenbank.org/>.
- [29] URM, "Ultima Risk Management," 2017. [Online]. Available: <http://www.ultimariskmanagement.com/>. [Accessed: 21-Jun-2017].
- [30] E. Humphreys, "Information security management standards: Compliance, governance and risk management," *Inf. Secur. Tech. Rep.*, vol. 13, no. 4, pp. 247–255, Nov. 2008.
- [31] A. Ambre and N. Shekokar, "Insider threat detection using log analysis and event correlation," in *Procedia Computer Science*, 2015, vol. 45, no. C, pp. 436–445.
- [32] R. Horne, "The cyber threat to banking: A Global Industry Challenge," *Pwc*, vol. 60, no. 2, p. 13, 2014.
- [33] Kaspersky Lab, "Banks Spend on IT Security is 3x Higher Than Non-Financial Organizations | Kaspersky Lab UK," 2017. [Online]. Available: https://www.kaspersky.co.uk/about/press-releases/2017_banks-spends. [Accessed: 17-Jul-2017].
- [34] C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," *Inf. Manag.*, vol. 51, no. 5, pp. 551–567, Jul. 2014.
- [35] I. Agrafiotis, A. Erola, J. Happa, M. Goldsmith, and S. Creese, "Validating an Insider Threat Detection System: A Real Scenario Perspective," in *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops*,

- SPW 2016*, 2016, pp. 286–295.
- [36] S. Dynes, E. Goetz, and M. Freeman, “Cyber security: Are economic incentives adequate?,” in *IFIP International Federation for Information Processing*, 2007, vol. 253, pp. 15–27.
- [37] Y. Wu, G. Feng, N. Wang, and H. Liang, “Game of information security investment: Impact of attack types and network vulnerability,” *Expert Syst. Appl.*, vol. 42, no. 15–16, pp. 6132–6146, Sep. 2015.
- [38] R. Von Solms and J. Van Niekerk, “From information security to cyber security,” *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.
- [39] R. Sumroy, N. Donovan, and R. McDonnell, “Cyber security – A real world issue,” 2014.
- [40] D. Clemente, “Cyber Security and Global Interdependence: What Is Critical?,” *Chatham House*, no. February, 2013.
- [41] J. Jang-Jaccard and S. Nepal, “A survey of emerging threats in cybersecurity,” in *Journal of Computer and System Sciences*, 2014, vol. 80, no. 5, pp. 973–993.
- [42] S. Mohurle and M. Patil, “A brief study of Wannacry Threat: Ransomware Attack 2017,” *Int. J. Adv. Res. Comput. Sci.*, vol. 8, no. 5, pp. 2016–2018, 2017.
- [43] P. R. Siddharth, “Stuxnet , A new Cyberwar weapon : Analysis from a technical point of view,” 2014.
- [44] M. E. O’Connell, “Cyber Security without Cyber War,” *J. Confl. Secur. Law*, vol. 17, no. 2, pp. 187–209, Jul. 2012.
- [45] C. James, “Cybersecurity Threats, Challenges and Opportunities,” *Australian Cyber Security*, no. November. Australian Computer Society, pp. 1–59, 2016.
- [46] R. Hummel and T. Baccam, “Securing Against the Most Common Vectors of Cyber Attacks,” 2017.
- [47] G. Disterer, “ISO/IEC 27000, 27001 and 27002 for Information Security

- Management," *J. Inf. Secur.*, vol. 04, no. 02, pp. 92–100, 2013.
- [48] A. D. "Veiga and J. H. P. . Eloff, "An information security governance framework," *Inf. Syst. Manag.*, vol. 24(4), pp. 361–372, 2007.
- [49] ISO, "The ISO Survey of Management System Standard Certifications 2016," vol. 16949, no. September, p. 2, 2017.
- [50] I. Luke, "The UK accounts for 10% of global ISO 27001 certifications and ranks second in the world," *IT Governance Blog*, 2017. [Online]. Available: <https://www.itgovernance.co.uk/blog/the-uk-accounts-for-10-of-global-iso-27001-certifications-and-ranks-second-in-the-world/>. [Accessed: 04-Apr-2018].
- [51] Ross, Ronald S, Johnson, and La, "NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems," 2014.
- [52] SSC, "PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2," 2015.
- [53] HealthIT.gov, "Guide to Privacy and Security of Health Information," 2013.
- [54] ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," 2013.
- [55] FDIC, "The Gramm-Leach-Bliley Act: Privacy of Consumer Financial Information," vol. 2000, no. January, pp. 1–28, 2001.
- [56] ISO/IEC 27001:2013, "Information technology - Security techniques - Specification for an Information Security Management System.," The British Standard Institute 2014, The British Standard Institute, 2014.
- [57] T. Fagade, "Hacking a Bridge: Information Security Risk Assessment of Smart Infrastructure (MSc Thesis)," University of Bristol, 2011.
- [58] US-CERT, "Build Security In. Governance and Management." Department of Homeland Security, Online, p. 08 Jan 2016, 2015.
- [59] C. Levy, E. Lamarre, and J. Twining, "Taking control of organizational risk

- culture," London, 2010.
- [60] C. "Vroom and R. . von Solms, "Towards information security behavioural compliance," *Comput.Secur.*, vol. 23(3), pp. 191–198, 2004.
- [61] E. "Sherif, S. Furnell, and N. . Clarke, "An identification of variables influencing the establishment of information security culture," in *"In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Tryfonas, T., Askoxylakis, I. (eds.),"* 2015, p. "vol. 9190, p. 436–448."
- [62] S. "Furnell and N. . Clarke, "'Organizational security culture: Embedding security awareness, education, and training,'" in *In: Proceedings of the IFIP TC11 WG*, 2005, p. "vol. 11, p. 67–74."
- [63] A. B. "Ruighaver, S. B. Maynard, and S. . Chang, "Organizational security culture: Extending the end-user perspective.," *Comput. Secur.*, vol. 26(1), pp. 56–62, 2007.
- [64] M. A. Alnatheer, "A Conceptual Model to Understand Information Security Culture," *Int. J. Soc. Sci. Humanit.*, vol. 4, no. 2, pp. 104–107, 2014.
- [65] S. M. Wu, D. Guo, and Y. C. Wu, "The Effects of Bank Employees' Information Security Awareness on Performance of Information Security Governance," in *Advances in Intelligent Systems and Computing*, Vol 686., Z. A. Khafa F., Patnaik S., Ed. Springer, Cham, 2018, pp. 657–663.
- [66] A. "Martins and J.. Elofe, "Information security culture," in *"In: Ghonaimy, M.A., El-Hadidi, M.T., Aslan, H.K. (eds.),"* 2002, pp. 203–214.
- [67] NITDA, "National Information Technology Development Agency: Guidelines on Data Protection," vol. <http://www>, p. Accessed 08 Jan 2016, 2013.
- [68] J. "Merete Hagen, E. Albrechtsen, and J. . Hovden, "Implementation and effectiveness of organizational information security measures," *Inf. Manag. Comput. Secur.*, vol. 16(4), pp. 377–397, 2008.

- [69] Valerie Vogel, "Effective Security Metrics," *Higher Ed Information Security Guide*, 2017. [Online]. Available: <https://spaces.internet2.edu/display/2014infosecurityguide/Effective+Security+Metrics>. [Accessed: 07-Dec-2017].
- [70] W. Jansen, "Directions in Security Metrics Research, NISTIR 7564," *Natl. Inst. Stand. Technol.*, vol. April, pp. 1–26, 2009.
- [71] I. Tashi and S. Ghernaouti-Hélie, "Security metrics to improve information security management," in *Proceedings of the 6th Annual Security Conferenceth Annual Security Conference*, 2007, pp. 47–1--47–13.
- [72] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Boston: Addison-Wesley, 2007.
- [73] S. M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," *IEEE Secur. Priv. Mag.*, vol. 4, no. 4, pp. 96–96, Jul. 2006.
- [74] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, "Economic Impacts of Rules- versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers," *IEEE Secur. Priv.*, vol. 14, no. 3, pp. 52–60, May 2016.
- [75] S. Aurigemma and R. Panko, "A composite framework for behavioral compliance with information security policies," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2011, pp. 3248–3257.
- [76] M. Siponen, M. Adam Mahmood, and S. Pahlila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, Mar. 2014.
- [77] O. . "Chima, "How Bank Insiders Connive with Fraudsters." This Day, Online, 2015.
- [78] L. . "Morgan, ""Nigerian bank IT worker on the run after £23.5m cyber heist,"" *IT Governance Blog*, vol. 2015, no. 18 December. 2014.

- [79] S. "Park, A. B. Ruighaver, S. B. Maynard, and A. . Ahmad, "Towards understanding deterrence: information security managers' perspective," in *"In: In Proceedings of the International Conference on IT Convergence and Security . Kim, K.J., Ahn, S.J. (eds.),"* 2011, p. 21–37.
- [80] J. "D'Arcy and T. . Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings.," *Eur. J. Inf. Syst.*, vol. 20(6), pp. 643–658, 2011.
- [81] M. "Theoharidou, S. Kokolakis, M. Karyda, and E. . Kiountouzis, "The insider threat to Information Systems and the effectiveness of ISO17799.," *Comput. Secur.*, vol. 24(6), pp. 472–484, 2005.
- [82] O. Buckley, J. R. C. Nurse, P. A. Legg, M. Goldsmith, and S. Creese, "Reflecting on the ability of enterprise security policy to address accidental insider threat," in *Proceedings - 4th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014 - Co-located with 27th IEEE Computer Security Foundations Symposium, CSF 2014 in the Vienna Summer of Logic 2014*, 2014, pp. 8–15.
- [83] R. "Alavi, S. Islam, and H. . Mouratidis, "A conceptual framework to analyze human factors of information security management system (ISMS) in organizations," in *"In: International Conference on Human Aspects of Information Security, Privacy, and Trust. Tryfonas, T., Askoxylakis, I. (eds.),"* 2014, p. "vol. 8533, p. 297–305."
- [84] J. D. "Wall, L. Iyer, S. A.F., and M. . Siponen, "Conceptualizing Employee Compliance and Non-compliance in Information Security Research: A Review and Research Agenda," in *Dewald Roode Information Security Workshop*, 2013.
- [85] E. . "Albrechtsen, "A qualitative study of users' view on information security.," *Comput.Secur.*, vol. "26(4)," pp. 276–289, 2007.
- [86] A. "Da Veiga and J. H. P. . Eloff, "A framework and assessment instrument for information security culture," *Comput. Secur.*, vol. 29(2), pp. 196–207, 2010.

- [87] C. . "Herley, "So long, and no thanks for the externalities: the rational rejection of security advice by users," in *In: Proceedings of the 2009 Workshop on New Security Paradigms Workshop*, 2009, p. 133–144. ACM.
- [88] GlobalSCAPE., "Protecting Digitalized Assets in Healthcare.," 2013.
- [89] S. Bauer and K. Chudzikowski, "Mind the Threat! A Qualitative Case Study on Information Security Awareness Programs in European Banks," *AMCIS 2015 Proc.*, 2015.
- [90] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future directions for behavioral information security research," *Comput. Secur.*, vol. 32, pp. 90–101, Feb. 2013.
- [91] Cert Insider Threat Center, "Unintentional Insider Threats: Social Engineering," vol. CMU/SEI-20, p. 109, 2014.
- [92] Matt Rosenquist, "Prioritizing Information Security Risks with Threat Agent Risk Assessment," 2009.
- [93] L. Marinos and A. Sfakianakis, "ENISA Threat Landscape - Responding to the Evolving Threat Environment," 2012.
- [94] J. Ophoff *et al.*, "A Descriptive Literature Review and Classification of Insider Threat Research," *Proc. Informing Sci. IT Educ. Conf. 2014*, vol. 2014, pp. 211–223, 2014.
- [95] Kowalski Dawn *et al.*, "Insider Threat Study: Illicit Cyber Activity in the Government Sector," 2008.
- [96] E. Kowalski and A. P. Moore, "Insider Threat Study : Illicit Cyber Activity in the Information Technology and Telecommunications Sector," 2008.
- [97] C. Colwill, "Human factors in information security: The insider threat – Who can you trust these days?," *Inf. Secur. Tech. Rep.*, vol. 14, no. 4, pp. 186–196, Nov. 2009.
- [98] K. Roy Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *Inf. Secur. Tech.*

- Rep.*, vol. 15, no. 3, pp. 112–133, 2010.
- [99] K.-K. R. Choo, “The cyber threat landscape: Challenges and future research directions,” *Comput. Secur.*, vol. 30, no. 8, pp. 719–731, Nov. 2011.
- [100] Q. Hu, R. West, L. Smarandescu, and Z. Yaple, “Why individuals commit information security violations: Neural correlates of decision processes and self-control,” in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2014, pp. 3234–3243.
- [101] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” *MIS Q.*, vol. 34, no. 3, pp. 523–548, 2010.
- [102] T. Herath and H. R. Rao, “Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness,” *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.
- [103] R. W. Rogers, “A Protection Motivation Theory of Fear Appeals and Attitude Change¹,” *J. Psychol.*, vol. 91, no. 1, pp. 93–114, Sep. 1975.
- [104] M. McBride, L. Carter, and M. Warkentin, “Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies,” in *The 2011 Dewald Roode Workshop on Information Systems Security Research*, 2012, pp. 1–13.
- [105] N. Liang and D. Biros, “Identifying Common Characteristics of Malicious Insiders,” in *Annual ADFSLS Conference on Digital Forensics, Security and Law*, 2015, no. 8, pp. 161–176.
- [106] US-CERT, “Combating the Insider Threat,” *Natl. Cybersecurity Commun. Integr. Cent.*, no. May, pp. 61–64, 2014.
- [107] I. Ajzen, “The theory of planned behavior,” *Organizational Behav. Hum. Decis. Process.*, vol. 50, no. 2, pp. 179–211, Dec. 1991.
- [108] N. Waly, R. Tassabehji, and M. Kamala, “Measures for improving

- information security management in organisations: the impact of training and awareness programmes," *UK Acad. Inf. Syst. Conf. Proc. 2012*, 2012.
- [109] T. Gundu and S. Flowerday, "Ignorance to awareness: Towards an information security awareness process," *SAIEE Africa Res. J.*, 2013.
- [110] R. L. Akers, "Rational choice, deterrence, and social learning theory in criminology: The path not taken," *J. Crim. Law Criminol.*, vol. 81, no. 3, pp. 653–676, 1990.
- [111] Q. Hu, Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?," *Commun. ACM*, vol. 54, no. 6, p. 54, Jun. 2011.
- [112] J. D'Arcy and T. Herath, "A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings," *Eur. J. Inf. Syst.*, vol. 20, no. 6, pp. 643–658, Nov. 2011.
- [113] S. Park, A. B. Ruighaver, S. B. Maynard, and A. Ahmad, "Towards understanding deterrence: Information security managers' perspective," in *Lecture Notes in Electrical Engineering*, 2012, vol. 23(3), pp. 21–37.
- [114] G. M. Sykes and D. Matza, "Techniques of Neutralization: A Theory of Delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, Dec. 1957.
- [115] Mikko Siponen and Anthony Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Q.*, vol. 34, no. 3, pp. 487–502, 2010.
- [116] M. Warkentin, M. McBride, L. Carter, A. Johnston, and A. C. Johnston, "The Role of Individual Characteristics on Insider Abuse Intentions," in *18th Americas Conference on Information Systems (AMCIS)*, 2012, no. 1, pp. 1–10.
- [117] Wikipedia, "Revised NEO Personality Inventory," 2012. [Online]. Available: https://en.wikipedia.org/wiki/Revised_NEO_Personality_Inventory.

[Accessed: 12-Aug-2017].

- [118] A. Cummings, T. Lewellen, D. McIntire, A. P. Moore, and R. Trzeciak, "Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector," 2012.
- [119] M. Kandias, A. Mylonas, N. Virvilis, M. Theoharidou, and D. Gritzalis, "An Insider Threat Prediction Model," in *TrustBus - International Conference on Trust, Privacy and Security in Digital Business*, 2010, pp. 26–37.
- [120] M. Kandias and V. Stavrou, "Proactive insider threat detection through social media: The YouTube case," in *Proceedings of the 12th ...*, 2013, pp. 261–266.
- [121] B. P. O'Connor and J. A. Dyce, "A test of models of personality disorder configuration.," *J. Abnorm. Psychol.*, vol. 107, no. 1, pp. 3–16, Feb. 1998.
- [122] B. Caci, M. Cardaci, M. E. Tabacchi, and F. Scrima, "Personality Variables as Predictors of Facebook Usage," *Psychol. Rep.*, vol. 114, no. 2, pp. 528–539, Apr. 2014.
- [123] A. Ortigosa, R. M. Carro, and J. I. Quiroga, "Predicting user personality by mining social interactions in Facebook," *J. Comput. Syst. Sci.*, vol. 80, no. 1, pp. 57–71, Feb. 2014.
- [124] B. Wood, "An insider threat model for adversary simulation," in *SRI International, Research on Mitigating the Insider Threat to Information Systems*, 2000, vol. 2, pp. 1–3.
- [125] E. T. Axelrad and P. J. Sticha, "A Bayesian Network Model for Predicting Insider Threats," in *Security and Privacy Workshops*, 2013, pp. 82–89.
- [126] P. Legg *et al.*, "Towards a conceptual model and reasoning structure for insider threat detection," *J. Wirel. Mob. Networks, Ubiquitous Comput. Dependable Appl.*, vol. 4, no. 4, pp. 20–37, 2013.
- [127] G. B. Magklaras and S. M. Furnell, "Insider threat prediction tool: Evaluating the probability of IT misuse," *Comput. Secur.*, vol. 21, no. 1,

- pp. 62–73, 1998.
- [128] S. Zeadally, B. Yu, D. H. Jeong, and L. Liang, “Detecting Insider Threats: Solutions and Trends,” *Inf. Secur. J. A Glob. Perspect.*, vol. 21, no. 4, pp. 183–192, Jan. 2012.
- [129] M. D. Back *et al.*, “Facebook profiles reflect actual personality, not self-idealization,” *Psychol. Sci.*, vol. 21, no. 3, pp. 372–374, Mar. 2010.
- [130] Y. Chen, S. Nyemba, W. Zhang, and B. Malin, “Leveraging Social Networks to Detect Anomalous Insider Actions in Collaborative Environments,” in *ISI ... : ... IEEE Intelligence and Security Informatics. ISI*, 2011, vol. 2011, pp. 119–124.
- [131] M. Kandias, K. Galbogini, L. Mitrou, and D. Gritzalis, “Insiders trapped in the mirror reveal themselves in social media,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2013, vol. 7873 LNCS, pp. 220–235.
- [132] S. Steele and C. Wargo, “An Introduction to Insider Threat Management,” *Inf. Syst. Secur.*, vol. 16, no. 1, pp. 23–33, Mar. 2007.
- [133] E. E. Schultz, “A framework for understanding and predicting insider attacks,” *Comput. Secur.*, vol. 21, no. 6, pp. 526–531, Oct. 2002.
- [134] F. L. Greitzer, D. A. Frincke, and M. Zabriskie, “Social/Ethical Issues in Predictive Insider Threat Monitoring,” in *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*, 2010, pp. 132–61.
- [135] F. L. Greitzer and D. A. Frincke, “Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation,” *Adv. Inf. Secur.*, vol. 49, pp. 85–113, 2010.
- [136] S.-C. Yang and Y.-L. Wang, “System Dynamics Based Insider Threats Modeling,” *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 3, 2011.
- [137] D. Vose, “Monte-Carlo risk analysis modelling,” in *Fundamentals of Risk*

- Analysis and Risk Management*, V. Molak, Ed. Boca Raton, Florida, USA.: CRC Press Inc, 1997, pp. 67–116.
- [138] B. M. J. Cerullo and V. Cerullo, “Threat Assessment and Security Measures Justification for Advanced IT Networks,” *Inf. Syst.*, vol. 1, pp. 1–9, 2005.
- [139] D. Danchev, “Building and implementing a successful information security policy,” *Wind. Com*, 2003.
- [140] S. Goel and V. Chen, “Information security risk analysis: A matrix based approach,” in *Proceedings of the Information Resource Management Association (IRMA) International Conference*, 2005, pp. 1–9.
- [141] M. Cobb, “Measuring Risk: A Security Pro’s Guide,” *Risk Management Tech Centre, Dark Reading*, 2012. [Online]. Available: <https://csbweb01.uncw.edu/people/cummingsj/classes/mis534/articles/Ch8MeasuringRisk.pdf>. [Accessed: 05-Feb-2017].
- [142] I. Bernik and K. Prislan, “Measuring information security performance with 10 by 10 model for holistic state evaluation,” *PLoS One*, vol. 11, no. 9, p. e0163050, Sep. 2016.
- [143] J. Lowder, “Risk Analysis: Why the ‘Risk = Threats x Vulnerabilities x Impact’ Formula is Mathematical Nonsense,” *BlogInfosec*, 2010. [Online]. Available: <https://www.bloginfosec.com/2010/08/23/why-the-risk-threats-x-vulnerabilities-x-impact-formula-is-mathematical-nonsense/>. [Accessed: 05-Apr-2017].
- [144] J. D. Hey, *Intermediate microeconomics*, 4th ed. McGraw-Hill, 2003.
- [145] Z. Yazar, “A Qualitative Risk Analysis and Management Tool - CRAMM,” 2002.
- [146] J. M. Woodruff, “Consequence and likelihood in risk estimation: A matter of balance in UK health and safety risk assessment practice,” *Saf. Sci.*, vol. 43, no. 5–6, pp. 345–353, Jun. 2005.
- [147] L. Anthony Cox, “What’s wrong with risk matrices?,” *Risk Anal.*, vol. 28,

- no. 2, pp. 497–512, Apr. 2008.
- [148] K. Wall, “The Trouble with Risk Matrices,” *Harv. Bus. Rev.*, vol. 87, no. 10, p. 16, 2009.
- [149] R. Anderson and T. Moore, “The economics of information security,” *Science*, vol. 314, no. 5799. American Association for the Advancement of Science, pp. 610–613, 27-Oct-2006.
- [150] M. J. Waller, G. P. Huber, and W. H. Glick, “Functional Background as A Determinant Of Executives’ Selective Perception,” *Acad. Manag. J.*, vol. 38, no. 4, pp. 943–974, Aug. 1995.
- [151] C. Berendonk, R. E. Stalmeijer, and L. W. T. Schuwirth, “Expertise in performance assessment: Assessors’ perspectives,” *Adv. Heal. Sci. Educ.*, vol. 18, no. 4, pp. 559–571, Oct. 2013.
- [152] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. Wiley Pub, 2008.
- [153] F. Farahmand, M. M. J. Atallah, and E. H. Spafford, “Incentive alignment and risk perception: An information security application,” *IEEE Trans. Eng. Manag.*, vol. 60, no. 2, pp. 238–246, May 2013.
- [154] R. Böhme, “Security metrics and security investment models,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6434 LNCS, pp. 10–24.
- [155] V. Franqueira, S. H. Houmb, and M. Daneva, “Using real option thinking to improve decision making in security investment,” in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2010, vol. 6426 LNCS, no. PART 1, pp. 619–638.
- [156] A. Mizzi, “Return on Information Security Investment - The Viability Of An Anti-Spam Solution In A Wireless Environment,” *Int. J. Netw. Secur.*, vol. 10, no. 1, pp. 18–24, 2010.

- [157] S.-L. Wang, J.-D. Chen, P. A. Stirpe, and T.-P. Hong, "Risk-neutral evaluation of information security investment on data centers," *J. Intell. Inf. Syst.*, vol. 36, no. 3, pp. 329–345, Jun. 2011.
- [158] S. Kokolakis, A. Kalliopi, and M. Karyda, "An analysis of privacy-related strategic choices of buyers and sellers in e-commerce transactions," in *Proceedings of the 2012 16th Panhellenic Conference on Informatics, PCI 2012*, 2012, pp. 123–126.
- [159] K. Anastasopoulou, T. Tryfonas, and S. Kokolakis, "Strategic Interaction Analysis of Privacy-Sensitive End-Users of Cloud-Based Mobile Apps," Springer, Berlin, Heidelberg, 2013, pp. 209–216.
- [160] L. Rajbhandari and E. A. Snekkenes, "Using game theory to analyze risk to privacy: An initial insight," in *IFIP Advances in Information and Communication Technology*, 2011, vol. 352 AICT, pp. 41–51.
- [161] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.
- [162] T. Spyridopoulos, I.-A. Topa, T. Tryfonas, and M. Karyda, "A Holistic Approach for Cyber Assurance of Critical Infrastructure with the Viable System Model," in *ICT Systems Security and Privacy Protection*, Springer, Berlin, Heidelberg, 2014, pp. 438–445.
- [163] T. Spyridopoulos, K. Maraslis, T. Tryfonas, G. Oikonomou, and S. Li, "Managing cyber security risks in industrial control systems with game theory and viable system modelling," in *Proceedings of the 9th International Conference on System of Systems Engineering: The Socio-Technical Perspective, SoSE 2014*, 2014, pp. 266–271.
- [164] H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security Patch Management: Share the Burden or Share the Damage?," *Manage. Sci.*, vol. 54, no. 4, pp. 657–670, Apr. 2008.
- [165] C. Derrick Huang, Q. Hu, and R. S. Behara, "An economic analysis of the optimal information security investment in the case of a risk-averse firm," *Int. J. Prod. Econ.*, vol. 114, no. 2, pp. 793–804, Aug. 2008.

- [166] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI) - A practical quantitative model," in *Journal of Research and Practice in Information Technology*, 2006, vol. 38, no. 1, pp. 45–56.
- [167] L. J. Tallau, M. Gupta, and R. Sharman, "Information security investment decisions: evaluating the Balanced Scorecard method," *Int. J. Bus. Inf. Syst.*, vol. 5, no. 1, p. 34, 2010.
- [168] D. Lyon, "Modeling Security Investments With Monte Carlo Simulations," 2014.
- [169] F. Baiardi, F. Corò, F. Tonelli, and D. Sgandurra, "Automating the assessment of ICT risk," *J. Inf. Secur. Appl.*, vol. 19, no. 3, pp. 182–193, Jul. 2014.
- [170] F. Baiardi and D. Sgandurra, "Assessing ICT risk through a Monte Carlo method," *Environ. Syst. Decis.*, vol. 33, no. 4, pp. 486–499, Dec. 2013.
- [171] S. M. H. Bamakan and M. Dehghanimohammadabadi, "A Weighted Monte Carlo Simulation Approach to Risk Assessment of Information Security Management System," *Int. J. Enterp. Inf. Syst.*, vol. 11, no. 4, pp. 63–78, Oct. 2015.
- [172] J. R. Conrad, P. Oman, and C. Taylor, "Managing Uncertainty in Security Risk Model Forecasts with RAPSA/MC," in *Security Management, Integrity, and Internal Control in Information Systems*, Boston: Kluwer Academic Publishers, 2005, pp. 141–156.
- [173] A. M. Colman, *Game theory and experimental games: The study of strategic interaction*. Elsevier, 2016.
- [174] E. Rasmusen, *Games and information : an introduction to game theory*. Blackwell Pub, 2007.
- [175] C. W. Probst, J. Hunker, D. Gollmann, and M. Bishop, "Insider threats in cyber security," *Adv. Inf. Secur.*, vol. 49, 2010.
- [176] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security

- management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no. 2, pp. 215–225, Apr. 2016.
- [177] C. Lee, C. C. Lee, and S. Kim, "Understanding information security stress: Focusing on the type of information security compliance activity," *Comput. Secur.*, vol. 59, pp. 60–70, Jun. 2016.
- [178] N. "Waly, R. Tassabehji, and M. . Kamala, "Measures for improving information security management in organisations: the impact of training and awareness programmes," in *In: Proceedings of the UK Academy for Information Systems Conference, 2012*, p. "Paper, 8."
- [179] T. "Gundu and S. V. Flowerday, "Ignorance to awareness: Towards an information security awareness process," *SAIEE Africa Res. J.*, vol. 104(2), pp. 69–79, 2013.
- [180] J. S. "Lim, A. Ahmad, S. Chang, and S. . Maynard, "Embedding information security culture emerging concerns and challenges," in *In: PACIS 2010 Proceedings, 2010*, p. Paper 43.
- [181] C. Posey, R. J. Bennett, and T. L. Roberts, "Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes," *Comput. Secur.*, vol. 30, no. 6–7, pp. 486–497, Sep. 2011.
- [182] E. Weishäupl, E. Yasasin, and G. Schryen, "Information security investments: An exploratory multiple case study on decision-making, evaluation and learning," *Computers and Security*, Elsevier Advanced Technology, 08-Feb-2018.
- [183] M. Balnaves and P. Caputi, *Introduction to quantitative research methods*. The University of Hong Kong, 2001.
- [184] J. C. Crisanto and J. Prenio, "Regulatory approaches to enhance banks' cyber-security frameworks," *Bank for International Settlements (BIS)*, Basel, Switzerland, 2017.
- [185] B. Kaplan and D. Duchon, "Combining Qualitative and Quantitative Methods in Information Systems Research: A Case Study," *MIS Q.*, vol. 12,

- no. 4, p. 571, Dec. 1988.
- [186] K. Kelley, B. Clark, V. Brown, and J. Sitzia, "Good practice in the conduct and reporting of survey research," *International Journal for Quality in Health Care*, vol. 15, no. 3. Oxford University Press, pp. 261–266, 01-May-2003.
- [187] A. Maria, "Introduction to Modelling and Simulation," in *Winter Simulation Conference*, 1997, pp. 7–13.
- [188] J. Creswell, *Educational research: Planning, conducting, and evaluating quantitative*, 4th ed. New York: Pearson, 2002.
- [189] R. K. Yin, *CASE STUDY RESEARCH: Design and Methods*, 2nd ed. Sage Publications, 1994.
- [190] S. Q. Qu and J. Dumay, "The Qualitative Research Interview," *Qual. Res. Account. Manag.*, vol. 8, no. 3, pp. 238–264, Aug. 2011.
- [191] Z. Zainal, "Case study as a research method," *J. Kemanus*, vol. 9, 2007.
- [192] R. K. Yin, *Applications of case study research*. Sage, 2011.
- [193] M. K. Malhotra and V. Grover, "An assessment of survey research in POM: from constructs to theory," *J. Oper. Manag.*, vol. 16, no. 4, pp. 407–425, Jul. 1998.
- [194] A. Pinsonneault and K. L. Kraemer, "Survey Research Methodology in Management Information Systems: An Assessment," *J. Manag. Inf. Syst.*, vol. 10, no. 2, pp. 75–105, 1993.
- [195] Verizon, "2017 Data Breach Investigations Report Tips on Getting the Most from This Report," 2017.
- [196] Ponemon Institute, "2017 Cost of Data Breach Study: Global Overview," 2017.
- [197] J. F. J. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, vol. 46, no. 1–2. 2014.
- [198] D. Zimmerman, "Model validation and verification of large and complex

- space structures," *Inverse Probl. Sci. Eng.*, vol. 8, no. 2, pp. 93–118, 2000.
- [199] BPS, "The British Psychological Society," 2018. [Online]. Available: <https://www.bps.org.uk/>. [Accessed: 01-Jul-2018].
- [200] FCA, "Cyber resilience - Financial Conduct Authority." [Online]. Available: <https://www.fca.org.uk/firms/cyber-resilience>. [Accessed: 03-Jul-2018].
- [201] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," *Natl. Inst. Stand. Technol.*, pp. 1–41, 2014.
- [202] J. Kwon and M. E. Johnson, "Security practices and regulatory compliance in the healthcare industry," *J. Am. Med. Informatics Assoc.*, vol. 20, no. 1, pp. 44–51, Jan. 2013.
- [203] J. Q. Wilson and G. L. Kelling, "Broken Windows," *Atl. Mon.*, vol. 249, no. 3, pp. 29–38, 1982.
- [204] MALCOLM GLADWELL, *The Tipping Point: How Little Things Can Make a Big Difference*, First. Boston: Little, Brown and Company, 2000.
- [205] S. Bauer and E. W. N. Bernroider, "From Information Security Awareness to Reasoned Compliant Action," *ACM SIGMIS Database DATABASE Adv. Inf. Syst.*, vol. 48, no. 3, pp. 44–68, Aug. 2017.
- [206] Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture," *Decis. Sci.*, vol. 43, no. 4, pp. 615–660, Aug. 2012.
- [207] Deloitte, "Insight into the Information Security Maturity of Organisations, with a Focus on Cyber Security," 2014.
- [208] W. L. (William L. Neuman, *Social research methods: qualitative and quantitative approaches*, 7th ed. Pearson Education, 2013.
- [209] A. "Da Veiga, N. Martins, and J. H. P. Eloff, "Information security culture - validation of an assessment instrument," *South. Afr. Bus. Rev.*, vol. 11(1), pp. 147–166, 2007.

- [210] G. M. Sullivan, A. R. Artino, and Jr, "Analyzing and interpreting data from likert-type scales," *J. Grad. Med. Educ.*, vol. 5, no. 4, pp. 541–2, Dec. 2013.
- [211] J. "Jackson, B. Bradford, M. Hough, A. Myhill, P. Quinton, and T. R. . Tyler, "Why do people comply with the law? Legitimacy and the influence of legal institutions," *Br. J. Criminol.*, vol. 52(6), pp. 1051–1071, 2012.
- [212] K. J. "Knapp, E. M. Thomas, R. Kelly, and F. . Nelson, "Information security: management's effect on culture and policy," *Inf.Manage. Comput. Secur.*, vol. 14(1), pp. 24–36, 2006.
- [213] B. Lebek, J. Uffen, M. Neumann, B. Hohler, and M. H. Breitner, "Information security awareness and behavior: A theory-based literature review," *Manag. Res. Rev.*, vol. 37, no. 12, pp. 1049–1092, Nov. 2014.
- [214] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014.
- [215] J. D'Arcy, A. Hovav, and D. Galletta, "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, Mar. 2009.
- [216] D. B. Cornish and R. V Clarke, "The reasoning criminal : rational choice perspectives on offending." New York : Springer-Verlag, 1986.
- [217] G. S. Becker, "Crime and Punishment: an Economic Approach," in *The Economic Dimensions of Crime*, London: Palgrave Macmillan UK, 1968, pp. 13–68.
- [218] C. R. Tittle, "Sanctions and social deviance: The question of deterrence," 1980.
- [219] K. Padayachee, "An Insider Threat Neutralisation Mitigation Model Predicated On Cognitive Dissonance (ITNMCD)," *South African Comput. J.*, vol. 56, no. 56, pp. 50–79, Jul. 2014.

- [220] M. R. Gottfredson and T. Hirschi, *A general theory of crime*. Stanford University Press, 1990.
- [221] R. Paternoster and S. Simpson, "Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime," *Law Soc. Rev.*, vol. 30, no. 3, p. 549, 1996.
- [222] G. M. Sykes and D. Matza, "Techniques of Neutralization: A Theory of Delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, p. 664, Dec. 1957.
- [223] R. Agnew and A. a. R. Peters, "Techniques of Neutralization," *Crim. Justice Behav.*, vol. 13, no. 6, pp. 81–97, Mar. 1986.
- [224] W. Li and L. Cheng, "Effects of Neutralization Techniques and Rational Choice Theory on Internet Abuse in the Workplace," in *PACIS 2013 Proceedings*, 2013.
- [225] J. Jackson, B. Bradford, M. Hough, A. Myhill, P. Quinton, and T. R. Tyler, "Why do people comply with the law? Legitimacy and the influence of legal institutions," *Br. J. Criminol.*, vol. 52, no. 6, pp. 1051–1071, Nov. 2012.
- [226] J. F. Hair, C. M. Ringle, and M. Sarstedt, "PLS-SEM: Indeed a Silver Bullet," *J. Mark. Theory Pract.*, vol. 19, no. 2, pp. 139–152, Apr. 2011.
- [227] D. George and P. Mallery, *IBM SPSS Statistics 23 step by step: A simple guide and reference*. 2016.
- [228] H. Latan and I. Ghozali, "Partial least squares: Concepts, techniques and application using program SmartPLS 3.0," 2015.
- [229] S. Bauer and E. W. N. Bernroider, "The effects of awareness programs on information security in banks: The roles of protection motivation and monitoring," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2015, vol. 9190, pp. 154–164.
- [230] G. M. Sykes and D. Matza, "Techniques of Nautralization: A Theory of Delinquency," *Am. Sociol. Rev.*, vol. 22, no. 6, pp. 664–670, 1957.

- [231] M. Merhi and V. Midha, "The impact of training and social norms on information security compliance: A pilot study," 2012.
- [232] D. D. Caputo, M. A. Maloof, and G. D. Stephens, "Detecting insider theft of trade secrets," *IEEE Secur. Priv.*, vol. 7, no. 6, pp. 14–21, 2009.
- [233] C. Melara, J.-M. Sarriequi, J. J. Gonzalez, A. Sawicka, and D. L. Cooke, "A System Dynamics Model of an Insider Attack on an Information System," *Proc. 2003 Syst. Dyn. Conf.*, no. October, pp. 9–36, 2003.
- [234] B. Schneier and Bruce, *Secrets and lies : digital security in a networked world*. John Wiley, 2000.
- [235] I. J. Martinez-Moyano, E. Rich, S. Conrad, D. F. Andersen, and T. R. Stewart, "A behavioral theory of insider-threat risks: A system dynamics approach," *ACM Trans. Model. Comput. Simul.*, vol. 18, no. 2, p. 7, 2008.
- [236] J. Golbeck, C. Robles, M. Edmondson, and K. Turner, "Predicting Personality from Twitter," in *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, 2011, pp. 149–156.
- [237] B. A. Alahmadi, P. A. Legg, and J. R. C. Nurse, "Using internet activity profiling for insider-threat detection," *ICEIS 2015 - 17th Int. Conf. Enterp. Inf. Syst. Proc.*, vol. 2, pp. 709–720, 2015.
- [238] S. Mehdizadeh, "Self-Presentation 2.0: Narcissism and Self-Esteem on Facebook," *Cyberpsychology, Behav. Soc. Netw.*, vol. 13, no. 4, pp. 357–364, Aug. 2010.
- [239] S. Malik and M. Khan, "Impact of facebook addiction on narcissistic behavior and self-esteem among students," *J. Pak. Med. Assoc.*, vol. 65, no. 3, pp. 260–3, Mar. 2015.
- [240] J. L. Skues, B. Williams, and L. Wise, "The effects of personality traits, self-esteem, loneliness, and narcissism on Facebook use among university students," *Comput. Human Behav.*, vol. 28, no. 6, pp. 2414–2419, Nov. 2012.

- [241] E. D. Shaw, K. Ruby, and J. Post, "The insider threat to information systems: The psychology of the dangerous insider," *Secur. Aware. Bull.*, vol. 2, no. 2, pp. 1–10, 1998.
- [242] I. Ajzen, "From Intentions to Actions: A Theory of Planned Behavior," in *Action Control*, Berlin, Heidelberg: Springer Berlin Heidelberg, 1985, pp. 11–39.
- [243]; Mehrpouyan H. Ackerman D, "Modeling human behavior to anticipate insider attacks via system dynamics," in *InProceedings of the Symposium on Theory of Modeling & Simulation 2016*, 2016, p. 3.
- [244] SANS, "The 6 Categories of Critical Log Information," *Security Laboratory*, 2013. [Online]. Available: <http://www.sans.edu/cyber-research/security-laboratory/article/sixtoplogcategories>. [Accessed: 02-Apr-2017].
- [245] K. O. McCabe and W. Fleeson, "Are traits useful? Explaining trait manifestations as tools in the pursuit of goals," *J. Pers. Soc. Psychol.*, vol. 110, no. 2, pp. 287–301, Feb. 2016.
- [246] OpenVAS, "OpenVAS - Open Vulnerability Assessment System: The world's most advanced Open Source vulnerability scanner and manager," *openvas.org*, 2016. [Online]. Available: <http://www.openvas.org/>. [Accessed: 12-Mar-2017].
- [247] Tenable Network Security, "Nessus Vulnerability Scanner," 2017. [Online]. Available: <https://www.tenable.com/products/nessus-vulnerability-scanner>. [Accessed: 12-Mar-2017].
- [248] Microsoft, "Microsoft Baseline Security Analyzer 2.3 (for IT Professionals)," 2017, 2017. [Online]. Available: <https://www.microsoft.com/en-us/download/details.aspx?id=7558>. [Accessed: 12-Mar-2017].
- [249] G. Stoneburner, A. Goguen, A. Feringa, and J. S. Hash, "Risk management guide for information technology systems," *NIST Spec. Publ. 800-30*, no. September 2001, 2002.

- [250] K. J. Soo Hoo, "How much is enough? A risk management approach to computer security," *Stanford Univ. USA*, no. June, p. 99, 2000.
- [251] R. Bojanc and B. Jerman-Blažič, "An economic modelling approach to information security risk management," *Int. J. Inf. Manage.*, vol. 28, no. 5, pp. 413–422, Oct. 2008.
- [252] E. Burtescu, "Decision Assistance in Risk Assessment – Monte Carlo Simulations," *Inform. Econ. vol. 16*, vol. 16, no. 4, pp. 86–93, 2012.
- [253] L. Xinhua, L. Yongzhi, and L. Hao, "Theory and Application of Monte Carlo Method," in *Software Engineering and Knowledge Engineering: Theory and Practice. Advances in Intelligent and Soft Computing*, vol. 115, Wu Y., Ed. Berlin, Heidelberg: Springer, Berlin, Heidelberg, 2012.
- [254] P. E. Johnson, *Monte Carlo Analysis in Academic Research*. Oxford University Press, 2013.
- [255] A. Calder and S. G. Watkins, *Information Security Risk Management for ISO27001-ISO27002*. Cambridgeshire: IT Governance Publishing, 2010.
- [256] J. Boltz, *Information Security Risk Assessment Practices of Leading Organizations, A Suppliment to GOA's May 1998 Executive Guide on Information Security Management*. Washinton, D.C: DIANE Publishing GOA/AIMD-00-33ions, 1999.
- [257] ENISA, "Introduction to Return on Security Investment: Helping CERTs Assessing the Cost of (Lack of) Security Investment," 2012. [Online]. Available: https://www.enisa.europa.eu/publications/introduction-to-return-on-security-investment/at_download/fullReport. [Accessed: 15-Apr-2016].
- [258] L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Commun. ACM*, vol. 49, no. 1, pp. 121–125, Jan. 2006.
- [259] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, "Economic Impacts of Rules-versus Risk-Based Cybersecurity Regulations for Critical Infrastructure Providers," *IEEE Secur. Priv.*, vol. 14, no. 3, pp. 52–60, May 2016.

- [260] L. A. (Tony) Cox, Jr., "Game Theory and Risk Analysis," *Risk Anal.*, vol. 29, no. 8, pp. 1062–1068, Aug. 2009.
- [261] R. Rue, S. L. Pfleeger, and D. Ortiz, "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making.," in *WEIS*, 2007, p. 23.
- [262] RiskAMP, "Risk Analysis Using Monte Carlo Simulation," 2016. [Online]. Available: [http://www.riskamp.com/files/Risk Analysis using Monte Carlo Simulation.pdf](http://www.riskamp.com/files/Risk_Analysis_using_Monte_Carlo_Simulation.pdf). [Accessed: 28-Jan-2016].
- [263] Ponemon Institute, "Cost of Data Breach Study: Global Analysis 2015 Cost of Data Breach Study: Global Analysis," 2015. [Online]. Available: <https://nhlearningsolutions.com/Portals/0/Documents/2015-Cost-of-Data-Breach-Study.PDF>. [Accessed: 14-Mar-2016].
- [264] Kaspersky Lab, "Damage Control: The Cost of Security Breaches, IT Security Risks Special Report Series," 2015. [Online]. Available: <http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-securitybreaches.%0Apdf>. [Accessed: 12-Mar-2016].
- [265] M. Van Hauwermeiren, D. Vose, and S. Vanden Bossche, "A Compendium of Distributions," *Vose Software, Ghent, Belgium*, 2012. [Online]. Available: <http://www.vosesoftware.com>. [Accessed: 29-Sep-2016].
- [266] D. M. Kammen and D. M. Hassenzahl, *Should we risk it? Exploring environmental, health, and technological problem solving*. New Jersey: Princeton University Press, 2001.
- [267] K. D. Tunnell, "Choosing crime: Close your eyes and take your chances," *Justice Q.*, vol. 7, no. 4, pp. 673–690, Dec. 1990.
- [268] R. Kissel, "Glossary of Key Information Security Terms Glossary of Key Information Security Terms," *Nist*, vol. NISTIR 729, no. Revision 2, 2013.

APPENDICES

APPENDIX I: CONCEPTS AND DEFINITIONS	217
APPENDIX II: INTERVIEW QUESTIONS.....	221
APPENDIX III: SURVEY QUESTIONS.....	222
APPENDIX IV: SURVEY MEASUREMENT MODEL - A	223
APPENDIX V: RECRUITMENT INFORMATION.....	224
APPENDIX VI: CLOSED ONLINE GOOGLE FORM.....	225
APPENDIX VII: SURVEY MEASUREMENT MODEL - B.....	226
APPENDIX VIII: IAAC 2016 POSTER.....	227
APPENDIX IX: CSW 2018 POSTER.....	228
APPENDIX X: THESIS TEMPLATE.....	229

APPENDIX I: CONCEPTS AND DEFINITIONS

It is necessary to clarify some terms, concepts and definitions used throughout this work as described in [7][8][57][45], and how the terms apply to information security risks within the scope of this thesis.

Accountability: Security objective that generates a requirement for the action of an entity to be uniquely traced to that entity at the individual level. It supports intrusion detection and prevention, non-repudiation, deterrence and fault isolation.

Administrator: Individual who has administrative access to the account and manages a computer system or network.

Assessment Method: This is one of the three types of action: examine, interview or test taken by assessors during an assessment in order to obtain evidence.

Asset: General support systems and high impact programs including personnel, mission-critical systems, equipment, physical plant or logically related group of systems.

Attack Attribution: The procedure or approach of determining, tracking and blaming the adversary that causes a cyber-attack or other security exploits.

Attack: Any malicious action that attempts to compromise system activities or gain unauthorised access to information resources and system services.

Availability: Protection of systems and data from intentional and accidental attempt to cause a denial of service, unauthorised deletion or unauthorised purposes. It is also about ensuring timely and reliable access to and use of information.

Baseline Security: Minimum level of security controls required for safeguarding an IT system against the threat of integrity, confidentiality and availability protection.

Black Hat: computer Programmers (Hacker) who exploit system vulnerabilities for personal or financial gain.

Business Continuity Plan (BCP): A document that describes a predetermined set of procedure, instructions and organisation plan of action to sustain any significant disruption to its mission/business functions.

Business Impact Analysis (BIA): Analysis of enterprise information system requirements, interdependencies and processes used to characterise contingency requirements and priorities in the case of disruption of significant scale.

Chief Information Security Officer (CISO): Organization official responsible for: 1) Providing advice to the head of the executive agency to ensure that information resources are managed and consistent with the requirements of legislation or industry Standards. 2) Develop, facilitate and maintain integrated information technology for the organisation.

Confidentiality: Preserving authorised restriction to sensitive information from individuals, entities or processes while it is in storage, being processed or in transit.

Control: Tools, processes, and measures put in place to reduce the impact of attack as a consequence of vulnerability exploitation.

Countermeasures: Techniques, processes, devices, actions and other measures that reduce, prevent or eliminate the vulnerability of an information system.

Critical Infrastructure: organisational or national assets (Physical and virtual) that are fundamental to its operations.

Cyberattack: An offensive act against computer systems, networks, or infrastructure.

Cybercrime: Computer-facilitated or technology-enabled violation of security.

Cyber Espionage: The practice and theft of confidential information from an individual or organisation.

Cybersecurity: The discipline and practice of preventing and mitigating attacks on computer systems and networks.

Cyberthreat: A potential threat targeting computer systems and technology, typically from the internet.

Cyberwarfare: Attack on computer systems, usually internet-based and perpetrated by the terrorist or political groups, or nation states to disrupt or destroy.

Exposure: Vulnerability without risk mitigating control.

Impact: The magnitude of harm that can occur as a consequence of unauthorised disclosure, modification, destruction of information or information system, and loss of availability.

Information Security Policy: Aggregate of direction, practices, rules and regulations that describe how an organisation distributes, protects and manages information.

Integrity: Ensuring systems remain operable throughout organisation life cycle by guarding against improper destruction and modification of information, including authentication and non-repudiation.

IoT: Internet of Things. Generic term for internet-connected devices like smartphones, lights, thermostats, and sensors.

Method: Process by which a threat agent attempts to exploit a vulnerability to accomplish a target.

Motivation: The Internal reason a threat agent needs to attack.

Objective: What the threat agent hopes to accomplish by the attack.

Risk Assessment: Part of risk management framework which identifies, prioritises and estimates risk as well as determines the impact of adverse circumstances on an enterprise.

Risk Mitigation: The evaluation, prioritisation and implementation of appropriate risk-reducing control based on the recommendation of risk assessment processes.

Risk: Information system-related security risks are the risks that arise from the loss of integrity, confidentiality and availability of information systems. It is a measure of the degree to which Information System is threatened based on the function of 1) the adverse impact of an event occurring and 2) the likelihood of the occurrence.

Threat Agent: Any person or entity who either with noxiousness or coincidentally starts attacks, to exploit vulnerabilities to create a loss.

Threat: Potential circumstances or event of an adverse impact on organisation, assets, individuals and operations as a result of unauthorised disclosure, destruction, access and modification of information, and denial of service.

Vulnerability: Part of information security infrastructure that could represent a weakness to attack without a control.

APPENDIX II: INTERVIEW QUESTIONS

Security compliance Interview

[University of Bristol Research Student]

These interview questions are to provide insight into the study of security compliance in banking organisations. Information collected is solely for this study and all data obtained will be entirely anonymised. Therefore, no individual respondent will be identified by this study.

Thank you for your participation.

Standard and Compliance Statements
1) Can you please tell me about your organisation security structure and procedure?
2) Can you describe your organisation security policy and guidelines?
3) What will you consider as the major contributing factor to your organisation's adoption of the ISO/IEC 27001 Standardisation?
4) What are the factors that can improve security compliance in your organisation?
5) What are the barriers to technical and procedural risk management in your organisation?

APPENDIX III: SURVEY QUESTIONS

Security compliance Survey

[University of Bristol Research Student]

This survey is to provide insight into the study of security compliance in banking organisations. Information collected is solely for this study and all data obtained will be entirely anonymised. Therefore, no individual respondent will be identified by this study.

Thank you for your participation.

Demography			
1) What is your job level/department in the organisation?			
Executive/Senior Level Manager		I.T Department	
HR & Administration		Other	
Operations			

The survey questions follow a Likert scale response model of strongly disagree, disagree, uncertain, agree and strongly agree. Please rate the following items on a scale of 1 to 5, with 1 being Strongly disagree and 5 being Strongly agree.

Security Culture Statements					
2) Information Security interferes with job productivity.	1	2	3	4	5
3) You can share your password with other people if you trust them.	1	2	3	4	5
4) It is safe to open an email attachment if it is not in the spam/junk box.	1	2	3	4	5
5) You can use personal digital devices and removable storage on your organisation computers.	1	2	3	4	5
6) You sometimes take official work home so that you can meet deadlines.	1	2	3	4	5
7) You can download/install software on your work computer within the corporate network.	1	2	3	4	5
8) You always lock your computer screen each time you leave your workstation.	1	2	3	4	5
Knowledge & Awareness Statements					
9) Your organisation has information security policy, and you know where to locate a copy.	1	2	3	4	5
10) Your organisation has provided security awareness and training to all employees.	1	2	3	4	5
11) You know how to identify and report suspicious/actual security breaches.	1	2	3	4	5
12) Information is permanently lost when files on hard drives are erased or formatted.	1	2	3	4	5

APPENDIX IV: SURVEY MEASUREMENT MODEL - A

Survey Measurement Model Part A

Construct	Measurement Item	Adopted Literature
Security Culture (Attitude and Compliant Behaviour)	Information Security interferes with job productivity	Hue et al. (2012)
	You can share your password with other people if you trust them.	
	It is safe to open an email attachment if it is not in the spam/junk box	
	You can use personal digital devices and removable storage on your organisation computers.	
	You sometimes take official work home so that you can meet deadlines.	
	You can download/install software on your work computer within the corporate network.	
	You always lock your computer screen each time you leave your workstation	
	Your organisation has information security policy, and you know where to locate a copy.	
Knowledge and Awareness	Your organisation has provided security awareness and training to all employees.	Deloitte: Central Asia Information Security Survey Result (2014)
	You know how to identify and report suspicious/actual security breaches.	
	Information is permanently lost when files on hard drives are erased or formatted.	

APPENDIX V: RECRUITMENT INFORMATION

Information Security Survey

Reply all | ▾

Delete

Junk | ▾

...

Information Security Survey

TF

Tesleem Fagade

Thu 28/01/2016 10:45

To: [REDACTED]

Bcc: [REDACTED] .gov.ng; r [REDACTED] om; yi [REDACTED] :om; ti [REDACTED] bank.com ↗

Sent Items

Morning, [REDACTED]

The link below is for the Information Security on-line survey discussed earlier.

<http://goo.gl/forms/rNDuRhMhd9>

This survey is designed to capture how organisations view, formulate, implement and maintain compliance to information security policies. We intend to sample employees awareness and how they respond to situations within the context of information security - including behaviour, trust, ethical conduct and change management. This is a pilot sample of a wider quantitative study in the field of information security culture. Respondents are anonymous, work place details and other sensitive data are not collected in this survey.

The survey has 12 multiple choice questions that can be completed in less than 5 minutes. Please answer all questions.

Thank you for your time.

Regards,

Tesleem Fagade
PhD Researcher
Dept. of Computer Science
University of Bristol

<https://outlook.office.com/owa/projection.aspx>

1/2

APPENDIX VI: CLOSED ONLINE GOOGLE FORM

The screenshot shows a Google Form titled "Information Security Survey" that is no longer accepting responses. The form has a purple header and a white message box in the center. The message states: "The form 'Information Security Survey' is no longer accepting responses. Try contacting the owner of the form if you think this is a mistake." Below the message box, there is a link to "Report Abuse - Terms of Service - Additional Terms". The Google Forms logo is visible at the bottom of the form. The URL at the bottom of the page is <https://docs.google.com/forms/d/1gPazb1FDo4BvVDGyXYc4zy9J9t-SUVPASa7DMEFIYrA/closedform>.

Information Security Survey

Information Security Survey

The form "Information Security Survey " is no longer accepting responses.

Try contacting the owner of the form if you think this is a mistake.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Additional Terms](#)

Google Forms


<https://docs.google.com/forms/d/1gPazb1FDo4BvVDGyXYc4zy9J9t-SUVPASa7DMEFIYrA/closedform> 1/1

APPENDIX VII: SURVEY MEASUREMENT MODEL - B

Survey Measurement Model Part B

Construct	Item		Adopted Literature
Personality Traits and Security Scenario Effect	LSS1	My internet access privileges are restricted by my organisation.	McBride et al. (2012) Wenli Li (2013)
	LSS2	Security violations are severely punished by my organisation.	
	LRE1	My organisation security policy is not stringent, I can get away with security violations.	
	LRE2	You can use personal digital devices and removable storage on your organisation computers.	
	LTV1	I intend to use organisation internet for non-work-related purposes	
	LTV2	There is a low chance of being caught if I use work computer for personal use.	
Neutralisation Techniques	DR1	You sometimes take official work home so that you can meet deadlines.	Hue et al. (2012) Siponen et al. (2014)
	DR2	It is Ok to violate security protocol if you don't understand it.	
	DI1	You can share your password with other people if you trust them.	
	DI2	Work stress is too high, and security interferes with job productivity.	
	BV1	You can download/install software on your work computer within the corporate network.	
	BV2	If managers are worried about security, they should have a better security management.	
Knowledge and Awareness	SC1	You always lock your computer screen each time you leave your workstation.	Survey Measurement Model Part A (Chapter 4)
	SC2	It is safe to open an email attachment if it is not in the spam/junk box.	
	KA1	Your organisation has provided security awareness and training to all employees.	
	KA2	You know how to identify and report suspicious/actual security breaches.	

APPENDIX VIII: IAAC 2016 POSTER



Cybersecurity Resource Allocation: The Monte Carlo Predictive Modelling Approach

Tesleem Fagade, Konstantinos Maraslis, Theo Tryfonas

Introduction

Information security is fundamentally concerned with the confidentiality, integrity and availability of information assets at all times. Organisations invest in countermeasures to defend against threats to information assets, however, as the number of assets to be protected grows and IT budgets are constrained, there is need for evaluation of information security investments. Security expenditure is a crucial resource allocation decision, yet little is known about the budgeting process used to justify how much to spend on information security.

Problem definition

Often, security budget decisions are a reflection of organisation threat tolerance, based on a risk scoring matrix. Traditionally, risk scoring matrix is calculated on the assumption that an event will happen given a probability of occurrence, and impact of threat. Security budget to mitigate risks is then allocated based on the resultant estimated risk score.


- Risk scoring formula is given as:

$$Risk = Probability (P) \times Impact (I)$$
- This approach assumes subjective probability estimation that is ambiguous and deterministic.
- In practice, it is difficult to apply this calculation to real world problems, in order to optimise resource allocation decisions.
- The sum of each deterministic estimate becomes the total cost estimate of security breach for the whole enterprise as shown in the table 1.

Aim of Research

This work explores how Monte-Carlo predictive simulation model can be used within the context of information security, for effective security investment decisions. Using verifiable historical cost from security breach reports in a conceptual enterprise scenario, the model is able to take into account the cost of potential breaches.

Scenario Assumptions




- Key information asset points are determined by the security team of an organisation.
- Report estimation of security breach costs is taken from the Ponemon Institute 2015 Cost of Data Breach Study and Kaspersky Lab (2015) IT Security Risks Special Report Series.

- Limitations of the costing methodology outlined in the studies are not validated nor described in this work.
- Minimum and maximum value of security breach is subject to expert elicitation.

Asset Class	Asset Name	Asset Value	Asset Criticality	Asset Exposure	Asset Impact	Asset Risk
Information Assets	Customer Data	100,000	High	High	High	High
	Employee Data	50,000	Medium	Medium	Medium	Medium
	Supplier Data	20,000	Low	Low	Low	Low
IT Assets	IT Infrastructure	150,000	High	High	High	High
	IT Applications	80,000	Medium	Medium	Medium	Medium
	IT Services	30,000	Low	Low	Low	Low
Physical Assets	Physical Infrastructure	120,000	High	High	High	High
	Physical Applications	60,000	Medium	Medium	Medium	Medium
	Physical Services	20,000	Low	Low	Low	Low

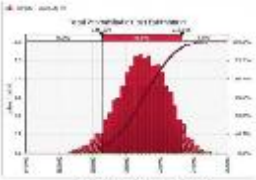
Methodology

- Firstly, uncertain fixed values in the model are identified and converted into ranges using a triangle distribution.
- Then uncertain cost values are defined as minimum (C_{min}), most likely (C_{ml}) and maximum (C_{max}) range of values, for each asset in the model calculations.
- Palisade @Risk software, a Monte Carlo simulation plugin for Microsoft Excel is used to generate 10,000 simulation runs.



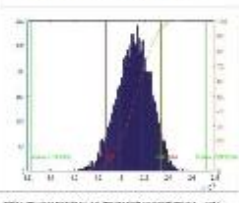
- Monte Carlo input variables are uncertain, random and defined according to a probability distribution.
- Thousands of scenarios are generated during simulation to reflect a probabilistic output for each uncertain input.
- The model output is a probabilistic range of costs and scenarios for optimal information security investment.

Result and Discussion



- Monte Carlo simulation adds extra dimension to the initial deterministic cost estimates.
- From the result in figure 3, it can be seen that the upper and the lower 5% represents extreme cases that is ignored by the simulation output.
- It can be seen that 90% of the simulation iterations fall under a value lower than the most likely estimated total values in table 2. Hence, we can say that 90% of the total cost of security a breach, will meet our initial estimate.

- While this is not a guarantee, it allows us to adjust IT security budget to reflect cost of potential breaches and also understand the risk that a budget may not meet initial estimates.
- @Risk result is validated with another simulation output in MATLAB as shown in figure 4.



- Further analysis of the result in figure 4 shows that given all iteration of simulation, the absolute minimum value of \$149,794 is much higher than the original deterministic minimum average value of \$123,000 (table 2). Similarly, the absolute maximum probabilistic value of \$253,700 is much lower than the deterministic value of \$272,000 after iteration, with only 5% chance of going over budget.
- The median point estimate is around the value of \$210,000 but from the result in figure 3, it can be seen that cost of impact could be significantly higher, possibly twice as high in terms of cumulative percentage.

Conclusion

This work demonstrated the application of Monte Carlo simulation to information security investment decision making.









- Deterministic point estimate of information security breach leads to subjective and erroneous cost evaluation.
- Probabilistic cost estimate captures uncertainty as a probability distribution, leading to objective range of values. However, as the complexity of asset class increases, using probabilistic estimates becomes difficult to manage.
- Monte Carlo simulation automates this process by testing each asset class as uncertain independent variable, and then computes thousands of scenarios for each set of uncertain variable.
- An information security risk assessor can derive confidence level in view of the best case, the most likely and the worst case scenarios.






Future work

Our model will be extended into how information security budget is fragmented, such that, information assets with the highest frequency and impact of threat are allocated more resources than those with low impact events.

References

- Wang, S. et al. (2011). Risk-neutral evaluation of information security investment on data centres. J of Intelligent Info Systems, 36(3), 329-345.
- Fouqueux, V. N. et al (2010). Using real option thinking to improve decision making in security investment. Springer Berlin Heidelberg.

APPENDIX IX: CSW 2018 POSTER

[illegible]

APPENDIX X: THESIS TEMPLATE

Thesis Template is downloaded from:

<https://www.scribd.com/document/294324944/csd-thesis-template-9th-draft-docx>